Security And Privacy In Internet Of Things Iots Models Algorithms And Implementations

Security and Privacy Issues in IoT Devices and Sensor Networks investigates security breach issues in IoT and sensor networks, exploring various solutions. The book follows a two-fold approach, first focusing on the fundamentals and theory surrounding sensor networks and IoT security. It then explores practical solutions that can be implemented to develop security for these elements, providing case studies to enhance understanding. Machine learning techniques are covered, as well as other security paradigms, such as cloud security and cryptocurrency technologies. The book highlights how these techniques can be applied to identify attacks and vulnerabilities, preserve privacy, and enhance data security. This in-depth reference is ideal for industry professionals dealing with WSN and IoT systems who want to enhance the security of these systems. Additionally, researchers, material developers and technology specialists dealing with the multifarious aspects of data privacy and security enhancement will benefit from the book's comprehensive information. Provides insights into the latest research trends and theory in the field of sensor networks and IoT security Presents machine learning-based solutions for data security enhancement Discusses the challenges to implement various security techniques Informs on how analytics can be used in security and privacy

With the immense amount of data that is now available online, security concerns have been an issue from the start, and have grown as new technologies are increasingly integrated in data collection, storage, and transmission. Online cyber threats, cyber terrorism, hacking, and other cybercrimes have begun to take advantage of this information that can be easily accessed if not properly handled. New privacy and security measures have been developed to address this cause for concern and have become an essential area of research within the past few years and into the foreseeable future. The ways in which data is secured and privatized should be discussed in terms of the technologies being used, the methods and models for security that have been developed, and the ways in which risks can be detected, analyzed, and mitigated. The Research Anthology on Privatizing and Securing Data reveals the latest tools and technologies for privatizing and securing data across different technologies and industries. It takes a deeper dive into both risk detection and mitigation, including an analysis of cybercrimes and cyber threats, along with a sharper focus on the technologies and methods being actively implemented and utilized to secure data online. Highlighted topics include information governance and privacy, cybersecurity, data protection, challenges in big data, security threats, and more. This book is essential for data analysts, cybersecurity professionals, data scientists, security analysts, IT specialists, practitioners, researchers, academicians, and students interested in the latest trends and technologies for privatizing and securing data.

This book provides a comprehensive study of the security and privacy research advancements in Internet of Things (IoT). The book lays the context for discussion by introducing the vulnerable intrinsic features of IoT. By providing a comprehensive discussion of the vulnerable features, the book highlights the problem areas of IoT related to security and privacy. - Covers all aspects of security - Algorithms, protocols and technologies used in IoT have been explained and the security flaws in them analyzed with solutions - Discusses ways for achieving better access control and trust in the IoT ecosystem - Contributes exhaustive strategic plans to deal with security issues of IoT - Gathers contributions from leading-edge researchers from academia and industry Graduates, researchers, people from the industry and security professionals who want to explore the IoT security field will find this book useful. The book will give an in-depth insight in to what has happened, what new is happening and what opportunities exist in the field.

The Internet of Things (IoT) has attracted strong interest from both academia and industry. Unfortunately, it has also attracted the attention of hackers. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations brings together some of the top IoT security experts from around the world who contribute their knowledg

Internet of Things From Hype to Reality

Achieving Privacy through Careful Design

Research Anthology on Privatizing and Securing Data

Security and Privacy Trends in the Industrial Internet of Things

The Road to Digitization

Security and Privacy Paradigm

Discusses how to set up defenses against hackers and online con artists, encryption methods, anonymizer software, spam, viruses, identity theft, firewalls, and ways to safeguard online purchases.

The Internet of Things (IoT), with its technological advancements and massive innovations, is building the idea of inter-connectivity among everyday life objects. With an explosive growth in the number of Internet-connected devices, the implications of the idea of IoT on enterprises, individuals, and society are huge. IoT is getting attention from both academia and industry due to its powerful real-time applications that raise demands to understand the entire spectrum of the field. However, due to increasing security issues, safeguarding the IoT ecosystem has become an important concern. With devices and information becoming more exposed and leading to increased attack possibilities, adequate security measures are required to leverage the benefits of this emerging concept. Internet of Things Security: Principles, Applications, Attacks, and Countermeasures is an extensive source that aims at establishing an understanding of the core concepts of IoT among its readers and the challenges and corresponding countermeasures in the field. Key features: Containment of theoretical aspects, as well as recent empirical findings associated with the underlying technologies Exploration of various challenges and trade-offs associated with the field and approaches to ensure security, privacy, safety, and trust across its key elements Vision of exciting areas for future research in the field to enhance the overall productivity This book is suitable for industrial professionals and practitioners, researchers, faculty members, and students across universities who aim to carry out research and development in the field of IoT 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.

Fully updated and revised, this leading guide on Internet privacy, anonymity and security contains all the practical information you need to inform and protect yourself. In this comprehensive yet easy-to-read guide for Windows users, you will quickly learn how to: stop search engines, social media and other powerful Internet players from tracking and profiling your online activities gain unrestricted access to all the content and downloads the Internet has to offer use social media to stay connected with friends in ways that don't compromise your privacy or safety keep hackers, identity thieves and adversaries from gaining access to your computer use the best (and often free!) privacy, anonymity and security apps that really work mask your IP address with a proxy, The Onion Router (Tor) or a virtual private network (VPN) use encryption to keep your digital items, downloads and personal information completely hidden and safe prevent surveillance and the monitoring of your activities by Internet service providers (ISP), governments, adversaries and other unwelcome snoops enjoy all the benefits (and downloads) of torrent file-sharing and Usenet newsgroups while staying protected and anonymous get rid of trace and hidden data on your computer that exposes your private activities conduct checks on how private your online activities and devices really are From your small investment in this book, you will benefit for years to come. After all, your privacy and security are priceless.

Understanding the Digital World

Successful IoT Device/Edge and Platform Security Deployment

Security Risk Management for the Internet of Things

A Commercial Law of Privacy and Security for the Internet of Things

Securing Privacy in the Internet Age

Cyber Privacy

Law of Internet Security and Privacy is the first legal guide to focus on critical issues of Internet security and privacy that affect businesses. This remarkably practical guide provides up-to-the-minute legal analysis and specific guidance to help combat deceptive online practices, protect privacy online, and avoid potentially devastating liability. You'll find the tools and information you need to respond effectively to universal security concerns such as viruses, backdoors and cryptography. The author analyzes the state of the law and sets forth clear guidelines on how to: Assess your system's risk against viruses Understand The uses of and problems with backdoors Develop essential security infrastructure Trap intruders Monitor employee use of computer/communications facilities Respond to claims against the employer resulting from misuse of the Internet Protect against unsolicited email (or spam) Untangle the bewildering array of regulations by different jurisdictions that influence e-commerce And The Internet. With its clear focus, rigorous legal analysis, and practical approach, Law of Internet Security and Privacy is an indispensable resource for key business decision makers and their counsel wrestling with emerging Internet privacy and security concerns.

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 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.

A brand-new edition of the popular introductory textbook that explores how computer hardware, software, and networks work Computers are everywhere. Some are highly visible, in laptops, tablets, cell phones, and smart watches. But most are invisible, like those in appliances, cars, medical equipment, transportation systems, power grids, and weapons. We never see the myriad computers that quietly collect, share, and sometimes leak personal data about us. Governments and companies increasingly use computers to monitor what we do. Social networks and advertisers know more about us than we should be comfortable with. Criminals have all-too-easy access to our data. Do we truly understand the power of computers in our world? In this updated edition of Understanding the Digital World, Brian Kernighan explains how computer hardware, software, and networks work. Topics include how computers are built and how they compute; what programming is; how the Internet and web operate; and how all of these affect security, privacy, property, and other important social, political, and economic issues. Kernighan touches on fundamental ideas from computer science and some of the inherent limitations of computers, and new sections in the book explore Python programming, big data, machine learning, and much more. Numerous color illustrations, notes on sources for further exploration, and a glossary explaining technical terms and buzzwords are included. Understanding the Digital World is a must-read for readers of all backgrounds who want to know more about computers and communications.

As society continues to rely heavily on technological tools for facilitating business, e-commerce, banking, and communication, among other applications, there has been a significant rise in criminals seeking to exploit these tools for their nefarious gain. Countries all over the world are seeing substantial increases in identity theft and cyberattacks, as well as illicit transactions, including drug trafficking and human trafficking, being made through the dark web internet. Sex offenders and murderers explore unconventional methods of finding and contacting their victims through Facebook, Instagram, popular dating sites, etc., while pedophiles rely on these channels to obtain information and photographs of children, which are shared on hidden community sites. As criminals continue to harness technological advancements that are outpacing legal and ethical standards, law enforcement and government officials are faced with the challenge of devising new and alternative strategies to identify and apprehend criminals to preserve the safety of society. The Encyclopedia of Criminal Activities and the Deep Web is a three-volume set that includes comprehensive articles covering multidisciplinary research and expert insights provided by hundreds of leading researchers from 30 countries including the United States, the United Kingdom, Australia, New Zealand, Germany, Finland, South Korea, Malaysia, and more. This comprehensive encyclopedia provides the most diverse findings and new methodologies for monitoring and regulating the use of online tools as well as hidden areas of the internet, including the deep and dark web. Highlighting a wide range of topics such as cyberbullying, online hate speech, and hacktivism, this book will offer strategies for the prediction and prevention of online criminal activity and examine methods for safeguarding internet users and their data from being tracked or stalked. Due to the techniques and extensive knowledge discussed in this publication it is an invaluable addition for academic and corporate libraries as well as a critical resource for policy makers, law enforcement officials, forensic scientists, criminologists, sociologists, victim advocates, cybersecurity analysts, lawmakers, government officials, industry professionals, academicians, researchers, and students within this field of study.

Powering the Internet of Things With 5G Networks

Encyclopedia of Criminal Activities and the Deep Web

Models, Algorithms, and Implementations

Smart Cities Cybersecurity and Privacy

Complete Guide to Internet Privacy, Anonymity & Security

Internet Security to Stop Big Companies from Tracking and Selling Your Data

```
Smart Cities Cybersecurity and Privacy examines the latest research developments and their outcomes for safe, secure, and trusting smart cities residents. Smart cities improve the quality
of life of citizens in their energy and water usage, healthcare, environmental impact, transportation needs, and many other critical city services. Recent advances in hardware and software,
have fueled the rapid growth and deployment of ubiquitous connectivity between a city's physical and cyber components. This connectivity however also opens up many security vulnerabilities
that must be mitigated. Smart Cities Cybersecurity and Privacy helps researchers, engineers, and city planners develop adaptive, robust, scalable, and reliable security and privacy smart
city applications that can mitigate the negative implications associated with cyber-attacks and potential privacy invasion. It provides insights into networking and security architectures,
designs, and models for the secure operation of smart city applications. Consolidates in one place state-of-the-art academic and industry research Provides a holistic and systematic
framework for design, evaluating, and deploying the latest security solutions for smart cities Improves understanding and collaboration among all smart city stakeholders to develop more
secure smart city architectures
This book provides a comprehensive study of the security and privacy research advancements in Internet of Things (IoT). The book lays the context for discussion by introducing the
vulnerable intrinsic features of IoT. By providing a comprehensive discussion of the vulnerable features, the book highlights the problem areas of IoT related to security and privacy. •
Covers all aspects of security • Algorithms, protocols and technologies used in IoT have been explained and the security flaws in them analyzed with solutions • Discusses ways for achieving
better access control and trust in the IoT ecosystem • Contributes exhaustive strategic plans to deal with security issues of IoT • Gathers contributions from leading-edge researchers from
academia and industry Graduates, researchers, people from the industry and security professionals who want to explore the IoT security field will find this book useful. The book will give
an in-depth insight in to what has happened, what new is happening and what opportunities exist in the field.
As organizations today are linking their systems across enterprise-wide networks and VPNs as well as increasing their exposure to customers, competitors, browsers and hackers on the
Internet, it becomes increasingly imperative for Web professionals to be trained in techniques for effectively protecting their sites from internal and external threats. Each connection
magnifies the vulnerability to attack. With the increased connectivity to the Internet and the wide availability of automated cracking tools, organizations can no longer simply rely on
operating system security to protect their valuable corporate data. Furthermore, the exploding use of Web technologies for corporate intranets and Internet sites has escalated security
risks to corporate data and information systems. Practical Internet Security reveals how the Internet is paving the way for secure communications within organizations and on the public
Internet. This book provides the fundamental knowledge needed to analyze risks to a system and to implement a security policy that protects information assets from potential intrusion,
damage, or theft. It provides dozens of real-life scenarios and examples, as well as hands-on instruction in securing Web communications and sites. You will learn the common vulnerabilities
of Web sites; as well as, how to carry out secure communications across unsecured networks. All system administrators and IT security managers will find this book an essential practical
resource.
An expert on computer privacy and security shows how we can build privacy into the design of systems from the start. We are tethered to our devices all day, every day, leaving data trails
of our searches, posts, clicks, and communications. Meanwhile, governments and businesses collect our data and use it to monitor us without our knowledge. So we have resigned ourselves to
the belief that privacy is hard--choosing to believe that websites do not share our information, for example, and declaring that we have nothing to hide anyway. In this informative and
illuminating book, a computer privacy and security expert argues that privacy is not that hard if we build it into the design of systems from the start. Along the way, Jaap-Henk Hoepman
debunks eight persistent myths surrounding computer privacy. The website that claims it doesn't collect personal data, for example; Hoepman explains that most data is personal, capturing
location, preferences, and other information. You don't have anything to hide? There's nothing wrong with wanting to keep personal information--even if it's not incriminating or
embarrassing--private. Hoepman shows that just as technology can be used to invade our privacy, it can be used to protect it, when we apply privacy by design. Hoepman suggests technical
fixes, discussing pseudonyms, leaky design, encryption, metadata, and the benefits of keeping your data local (on your own device only), and outlines privacy design strategies that system
designers can apply now.
Practical Internet of Things Security
Architectures and Security Measures
Demystifying Internet of Things Security
Security and Privacy Issues in IoT Devices and Sensor Networks
Technologies and Techniques for IoT Security, Privacy and Data Protection
Law of Internet Security and Privacy
```

This book presents a systematic and comprehensive overview for IoT security. It first introduces architecture approaches for IoT and IoT security, describing the security techniques for different layers in the IoT security architecture. It also provides an in-depth analysis on the difference between IoT security and traditional system and data security. It is commonly known that information security includes data confidentiality, data integrity, and availability, and that measures include non-repudiation and access control. However, in practical IoT system construction, many more security measures need to be carefully considered. As such, this book presents around 60 different security measures, mainly focusing on the sensor layer of IoT. These security measures can serve as a source of reference for IoT system construction, as well as IoT security standard making.

Securing the Internet of Things provides network and cybersecurity researchers and practitioners with both the theoretical and practical knowledge they need to know regarding security in the Internet of Things (IoT). This booming field, moving from strictly research to the marketplace, is advancing rapidly, yet security issues abound. This book explains the fundamental concepts of IoT security, describing practical solutions that account for resource limitations at IoT end-node, hybrid network architecture, communication protocols, and application characteristics. Highlighting the most important potential IoT security risks and threats, the book covers both the general theory and practical implications for people working in security in the

Internet of Things. Helps researchers and practitioners understand the security architecture in IoT and the state-of-the-art in IoT security countermeasures Explores how the threats in IoT are different from traditional ad hoc or infrastructural networks Provides a comprehensive discussion on the security challenges and solutions in RFID, WSNs, and IoT Contributed material by Dr. Imed Romdhani

How the enabling technologies in 5G as an integral or as a part can seamlessly fuel the IoT revolution is still very challenging. This book presents the state-of-the-art solutions to the theoretical and practical challenges stemming from the integration of 5G enabling technologies into IoTs in support of a smart 5G-enabled IoT paradigm, in terms of network design, operation, management, optimization, privacy and security, and applications. In particular, the technical focus covers a comprehensive understanding of 5G-enabled IoT architectures, converged access networks, privacy and security, and emerging applications of 5G-eabled IoT.

This book provides an overview of the most recent developments in Internet of Things (IoT) security and data protection. It presents the results of several international research projects addressing this topic from complementary angles. It starts by analyzing the main privacy and security threats on IoT, as well as the evolution of data protection norms, such as the European General Data Protection Regulation (GDPR), and their impact on IoT. Through a comprehensive and systematic approach, the contributors present new perspectives on IoT & Cloud Computing security requirements. They discuss the most recent approach to support trusted IoT, including new models of privacy risk assessment, labeling and certification, and contractual tools (such as Privacy PACT). Practical implementations, such as in the European Large Scale Pilots on IoT for Smart Cities (Synchronicity), are presented, explaining how they address security, privacy and data protection. Finally, innovative models to secure IoT systems are presented for the network and end-nodes security, including network threats analysis.

Internet Security Made Easy
The Complete Idiot's Guide to Internet Privacy and Security
5G-Enabled Internet of Things
Security and Privacy in the Internet of Things
A Beginner's Guide to Internet of Things Security
Security and Privacy in Internet of Things (Iots)

Going beyond current books on privacy and security, Unauthorized Access: The Crisis in Online Privacy and Security proposes specific solutions to public policy issues pertaining to online privacy and security. Requiring no technical or legal expertise, the book explains complicated concepts in clear, straightforward language. The authors—two renowned experts on computer security and law—explore the well-established connection between social norms, privacy, security, and technological structure. This approach is the key to understanding information security and informational privacy, providing a practical framework to address ethical and legal issues. The authors also discuss how rapid technological developments have created novel situations that lack relevant norms and present ways to develop these norms for protecting informational privacy and ensuring sufficient information security. Bridging the gap among computer scientists, economists, lawyers, and public policy makers, this book provides technically and legally sound public policy guidance about online privacy and security. It emphasizes the need to make trade-offs among the complex concerns that arise in the context of online privacy and security.

A Beginner's Guide to Internet of Things Security focuses on security issues and developments in the Internet of Things (IoT) environment. The wide-ranging applications of IoT, including home appliances, transportation, logistics, healthcare, and smart cities, necessitate security applications that can be applied to every domain with minimal cost. IoT contains three layers: application layer, middleware layer, and perception layer. The security problems of each layer are analyzed separately to identify solutions, along with the integration and scalability issues with the cross-layer architecture of IoT. The book discusses the state-of-the-art authentication-based security schemes, which can secure radio frequency identification (RFID) tags, along with some security models that are used to verify whether an authentication scheme is secure against any potential security risks. It also looks at existing authentication schemes and security models with their strengths and weaknesses. The book uses statistical and analytical data and explains its impact on the IoT field, as well as an extensive literature survey focusing on trust and privacy problems. The open challenges and future research direction discussed in this book will help to further academic researchers and industry professionals in the domain of security. Dr. Brij B. Gupta is an assistant professor in the Department of Computer Engineering, National Institute of Technology, Kurukshetra, India. Ms. Aakanksha Tewari is a PhD Scholar in the Department of Computer Engineering, National Institute of Technology, Kurukshetra, India.

This book, written by leaders in the protection field of critical infrastructures, provides an extended overview of the technological and operative advantages together with the security problems and challenges of the new paradigm of the Internet of Things in today's industry, also known as the Industry Internet of Things (IIoT). The incorporation of the new embedded technologies and the interconnected networking advances in the automation and monitoring processes, certainly multiplies the functional complexities of the underlying control system, whilst increasing security and privacy risks. The critical nature of the application context and its relevance for the well-being of citizens and their economy, attracts the attention of multiple, advanced attackers, with stealthy abilities to evade security policies, ex-filter information or exploit vulnerabilities. Some real-life events and registers in CERTs have already clearly demonstrated how the control industry can become vulnerable to multiple types of advanced threats whose focus consists in hitting the safety and security of the control processes. This book, therefore, comprises a detailed spectrum of research papers with highly analytical content and actuation procedures to cover the relevant security and privacy issues such as data protection, awareness, response and resilience, all of them working at optimal times. Readers will be able to comprehend the construction problems of the fourth industrial revolution and are introduced to effective, lightweight protection solutions which can be integrated as part of the new IIoT-based monitoring ecosystem.

With the rise of mobile and wireless technologies, more sustainable networks are necessary to support such communications. These next generation networks can now be utilized to strengthen the growing era of the Internet of Things. Powering the Internet of Things With 5G Networks is a comprehensive reference source for the latest scholarly research on the progression and design of fifth generation networks and their role in supporting the Internet of Things. Including a range of perspectives on topics such as privacy and security, large scale monitoring, and scalable architectures, this book is ideally designed for technology developers, academics, researchers, and practitioners interested in the convergence of the Internet of Things and 5G networks.

Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS)
Firewalls Don't Stop Dragons
Architectures, Techniques, and Applications
What You Need to Know about Computers, the Internet, Privacy, and Security, Second Edition
Internet of Things Security and Data Protection
The Crisis in Online Privacy and Security

Security, privacy, and trust in the Internet of Things (IoT) and CPS (Cyber-Physical Systems) are different from conventional security as concerns revolve around the collection and aggregation of data or transmission of data over the network. Analysis of cyber-attack vectors and the provision of appropriate mitigation techniques are essential research areas for these systems. Adoption of best practices and maintaining a balance between ease of use and security are, again, crucial for the effective performance of these systems. Recent Advances in Security, Privacy and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS) discusses and presents techniques and methodologies, as well as a wide range of examples and illustrations, to effectively show the principles, algorithms, challenges, and applications of security, privacy, and trust for IoT and CPS. Book features: Introduces new directions for research, development, and engineering security, privacy, and trust of IoT and CPS Includes a wealth of examples and illustrations to effectively demonstrate the principles, algorithms, challenges, and applications Covers most of the important security aspects and current trends not present in other reference books This book will also serve as an excellent reference in security, privacy, and trust of IoT and CPS for professionals in this fast-evolving and critical field. The chapters present high-quality contributions from researchers, academics, and practitioners from various national and international organizations and universities.

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 is a book about what privacy is and why it matters. Governments and companies keep telling us that Privacy is Dead, but they are wrong. Privacy is about more than just whether our information is collected. It's about what we do with that information. And in our modern society, that's pretty much everything we do, from GPS mapping to texting to voting to treating disease. We need to realize that privacy is up for grabs, and we need to craft rules to protect ourhard-won, but fragile human values like identity, freedom, consumer protection, and trust. Author Neil Richards shows what privacy is, why privacy matters, and how we can build a better digital future together.

Rely on this practical, end-to-end guide on cyber safety and online security written expressly for a non-technical audience. You will have just what you need to protect yourself—step by step, without judgment, and with as little jargon as possible. Just how secure is your computer right now? You probably don't really know. Computers and the Internet have revolutionized the modern world, but if you're like most people, you have no clue how these things work and don't know the real threats. Protecting your computer is like defending a medieval castle. While moats, walls, drawbridges, and castle guards can be effective, you'd go broke trying to build something dragon-proof. This book is not about protecting yourself from a targeted attack by the NSA: it's about armoring yourself against common hackers and mass surveillance. There are dozens of no-brainer things we all should be doing to protect our computers and safeguard our data—just like wearing a seat belt, installing smoke alarms, and putting on sunscreen. Author Carey Parker has structured this book to give you maximum benefit with minimum effort. If you just want to know what to do, every chapter has a complete checklist with step-by-step instructions and pictures. The book contains more than 150 tips to make you and your family safer. It includes: Added steps for Windows 10 (Spring 2018) and Mac OS X High Sierra Expanded coverage on mobile device safety Expanded coverage on safety for kids online More than 150 tips with complete step-by-step instructions and pictures What You'll Learn Solve your password problems once and for all Browse the web safely and with confidence Block online tracking and dangerous ads Choose the right antivirus software for you Send files and messages securely Set up secure home networking Conduct secure shopping and banking online Lock down social media accounts Create automated backups of all your devices Manage your home computers Use your smartphone and tablet safely Safeguard your kids online And more! Who This Book Is For Those who use computers and mobile devices, but don't really know (or frankly care) how they work. This book is for people who just want to know what they need to do to protect themselves—step by step, without judgment, and with as little jargon as possible. Attacks, Applications, Authentication, and Fundamentals

Who Has Your Data and Why You Should Care
Security and Privacy in Internet of Things (IoTs)
IoT
Principles, Applications, Attacks, and Countermeasures

In the Internet of Things (IoT) era, online activities are no longer limited to desktop or laptop computers, smartphones and tablets. Instead, these activities now include ordinary tasks, such as using an internet-connected refrigerator or washing machine. At the same time, the IoT provides unlimited opportunities for household objects to serve as surveillance devices that continually monitor, collect and process vast quantities of our data. In this work, Stacy-Ann Elvy critically examines the consumer ramifications of the IoT through the lens of commercial law and privacy and security law. The book provides concrete legal solutions to remedy inadequacies in the law that will help usher in a more robust commercial law of privacy and security that protects consumer interests.

A compelling argument that the Internet of things threatens human rights and security "Sobering and important."--Financial Times, "Best Books of 2020: Technology" 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 loss of communication but also potentially in 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 the 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.

In recent years, the rising complexity of Internet of Things (IoT) systems has increased their potential vulnerabilities and introduced new cybersecurity challenges. In this context, state of the art methods and technologies for security risk assessment have prominent limitations when it comes to large scale, cyber-physical and interconnected IoT systems. Risk assessments for modern IoT systems must be frequent, dynamic and driven by knowledge about both cyber and physical assets. Furthermore, they should be more proactive, more automated, and able to leverage information shared across IoT value chains. This book introduces a set of novel risk assessment techniques and their role in the IoT Security risk management process. Specifically, it presents architectures and platforms for end-to-end security, including their implementation based on the edge/fog computing paradigm. It also highlights machine learning techniques that boost the automation and proactiveness of IoT security risk assessments. Furthermore, blockchain solutions for open and transparent sharing of IoT security information across the supply chain are introduced. Frameworks for privacy awareness, along with technical measures that enable privacy risk assessment and boost GDPR compliance are also presented. Likewise, the book illustrates novel solutions for security certification of IoT systems, along with techniques for IoT security interoperability. In the coming years, IoT security will be a challenging, yet very exciting journey for IoT stakeholders, including security experts, consultants, security research organizations and IoT solution providers. The book provides knowledge and insights about where we stand on this journey. It also attempts to develop a vision for the future and to help readers start their IoT Security efforts on the right foot.

"Chilling, eye-opening, and timely, Cyber Privacy makes a strong case for the urgent need to reform the laws and policies that protect our personal data. If your reaction to that statement is to shrug your shoulders, think again. As April Falcon Doss expertly explains, data tracking is a real problem that affects every single one of us on a daily basis." —General Michael V. Hayden, USAF, Ret., former Director of CIA and NSA and former Principal Deputy Director of National Intelligence You're being tracked. Amazon, Google, Facebook, governments. No matter who we are or where we go, someone is collecting our data: to profile us, target us, assess us; to predict our behavior and analyze our attitudes; to influence the things we do and buy—even to impact our vote. If this makes you uneasy, it should. We live in an era of unprecedented data aggregation, and it's never been more difficult to navigate the trade-offs between individual privacy, personal convenience, national security, and corporate profits. Technology is evolving quickly, while laws and policies are changing slowly. You shouldn't have to be a privacy expert to understand what happens to your data. April Falcon Doss, a privacy expert and former NSA and Senate lawyer, has seen this imbalance in action. She wants to empower individuals and see policy catch up. In Cyber Privacy, Doss demystifies the digital footprints we leave in our daily lives and reveals how our data is being used—sometimes against us—by the private sector, the government, and even our employers and schools. She explains the trends in data science, technology, and the law that impact our everyday privacy. She tackles big questions: how data aggregation undermines personal autonomy, how to measure what privacy is worth, and how society can benefit from big data while managing its risks and being clear-eyed about its cost. It's high time to rethink notions of privacy and what, if anything, limits the power of those who are constantly watching, listening, and learning about us. This book is for readers who want answers to three questions: Who has your data? Why should you care? And most important, what can you do about it?

Privacy Is Hard and Seven Other Myths
A Step-by-Step Guide to Computer Security for Non-Techies
The Internet in Everything
Practical Internet Security
Why Privacy Matters
Securing the Internet of Things

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

The Internet of Things (IoT) has attracted strong interest from both academia and industry. Unfortunately, it has also attracted the attention of hackers. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations brings together some of the top IoT security experts from around the world who contribute their knowledge regarding different IoT security aspects. It answers the question How do we use efficient algorithms, models, and implementations to cover the four important aspects of IoT security, i.e., confidentiality, authentication, integrity, and availability? The book consists of five parts covering attacks and threats, privacy preservation, trust and authentication, IoT data security, and social awareness. The first part introduces all types of IoT attacks and threats and demonstrates the principle of countermeasures against those attacks. It provides detailed introductions to specific attacks such as malware propagation and Sybil attacks. The second part addresses privacy-preservation issues related to the collection and distribution of data, including medical records. The author uses smart buildings as an example to discuss privacy-protection solutions. The third part describes different types of trust models in the IoT infrastructure, discusses access control to IoT data, and provides a survey of IoT authentication issues. The fourth part emphasizes security issues during IoT data computation. It introduces computational security issues in IoT data processing, security design in time series data aggregation, key generation for data transmission, and concrete security protocols during data access. The fifth and final part considers policy and human behavioral features and covers social-context-based privacy and trust design in IoT platforms as well as policy-based informed consent in the Internet of Things.
Security and Privacy in the Internet of ThingsCRC Press

Your data has already been sold... Get it back. There are so many times when we are online, and we need to make sure that our data is safe. We assume that we are doing a good job with a bit of anti-virus protection and carefully selecting what sites we visit. But when some of the big companies we trust, including Facebook, Google, and more, are willing to gather up as much data as they can about all our lives (whether online or not) and then sell it and make money, it's hard to know how safe our information really is. This book is going to help you prevent that. While it may be difficult to keep this from happening, there are quite a few powerful steps that you can take. These help to keep the hackers out and will stop Google, Bing, and other companies from tracking you and will keep all your personal information nice and safe. It is amazing how much information companies are able to store about us and sell. Most are willing to

hand it over because we don't even realize it is happening; we are just following instructions and typing what we are prompted to type. Taking the proper precautions ahead of time can make life a little easier and put you back in the drivers' seat when it comes to keeping your data safe. This book will go through some of the simple steps you can take to keep your information safe and ensure that no one can take your data without your permission again. Some of the things YOU WILL LEARN: The TOP FIVE big companies already taking your information and selling it for mega-profits. The biggest SOCIAL MEDIA MISTAKES you need to fix, right now. The BEST HARDWARE to keep the trackers, and the hackers, out. The minimum MUST HAVE SOFTWARE that will lock down your system. How to SHUT DOWN HACKERS while you browse safely online. BULLETPROOF YOUR EMAIL and shop online without a care in the world. Safe online banking with these SECRET CREDIT CARDS. How to DELETE YOURSELF from the internet in under five minutes. While there are many ways that companies can take your data and use it for their own benefit, there are just as many ways for you to kick them out and gain control again. Some of the controls are right in front of your eyes provided to you by the companies themselves, and some will require you to take additional steps on your own. Regardless, it is worth considering using privacy controls to protect yourself and your data. Take back control of your data. Scroll up and click Buy Now.

The Right to Privacy
Security and Privacy in the Internet of Things: Challenges and Solutions
A Plain-English Guide to Protecting Yourself and Your Company Online
Internet of Things Security
Unauthorized Access
Digital Privacy

IOT: Security and Privacy Paradigm covers the evolution of security and privacy issues in the Internet of Things (IoT). It focuses on bringing all security and privacy related technologies into one source, so that students, researchers, and practitioners can refer to this book for easy understanding of IoT security and privacy issues. This edited book uses Security Engineering and Privacy-by-Design principles to design a secure IoT ecosystem and to implement cyber-security solutions. This book takes the readers on a journey that begins with understanding the security issues in IoT-enabled technologies and how it can be applied in various aspects. It walks readers through engaging with security challenges and builds a safe infrastructure for IoT devices. The book helps readers gain an understanding of security architecture through IoT and describes the state of the art of IoT countermeasures. It also differentiates security threats in IoT-enabled infrastructure from traditional ad hoc or infrastructural networks, and provides a comprehensive discussion on the security challenges and solutions in RFID, WSNs, in IoT. This book aims to provide the concepts of related technologies and novel findings of the researchers through its chapter organization. The primary audience includes specialists, researchers, graduate students, designers, experts and engineers who are focused on research and security related issues. Souvik Pal, PhD, has worked as Assistant Professor in Nalanda Institute of Technology, Bhubaneswar, and JIS College of Engineering, Kolkata (NAAC "A" Accredited College). He is the organizing Chair and Plenary Speaker of RICE Conference in Vietnam; and organizing co-convener of ICICIT, Tunisia. He has served in many conferences as chair, keynote speaker, and he also chaired international conference sessions and presented session talks internationally. His research area includes Cloud Computing, Big Data, Wireless Sensor Network (WSN), Internet of Things, and Data Analytics. Vicente García-Díaz, PhD, is an Associate Professor in the Department of Computer Science at the University of Oviedo (Languages and Computer Systems area). He is also the editor of several special issues in prestigious journals such as Scientific Programming and International Journal of Interactive Multimedia and Artificial Intelligence. His research interests include eLearning, machine learning and the use of domain specific languages in different areas. Dac-Nhuong Le, PhD, is Deputy-Head of Faculty of Information Technology, and Vice-Director of Information Technology Apply and Foreign Language Training Center, Haiphong University, Vietnam. His area of research includes: evaluation computing and approximate algorithms, network communication, security and vulnerability, network performance analysis and simulation, cloud computing, IoT and image processing in biomedical. Presently, he is serving on the editorial board of several international journals and has authored nine computer science books published by Springer, Wiley, CRC Press, Lambert Publication, and Scholar Press.

Break down the misconceptions of the Internet of Things by examining the different security building blocks available in Intel Architecture (IA) based IoT platforms. This open access book reviews the threat pyramid, secure boot, chain of trust, and the SW stack leading up to defense-in-depth. The IoT presents unique challenges in implementing security and Intel has both CPU and Isolated Security Engine capabilities to simplify it. This book explores the challenges to secure these devices to make them immune to different threats originating from within and outside the network. The requirements and robustness rules to protect the assets vary greatly and there is no single blanket solution approach to implement security. Demystifying Internet of Things Security provides clarity to industry professionals and provides and overview of different security solutions What You'll Learn Secure devices, immunizing them against different threats originating from inside and outside the networkGather an overview of the different security building blocks available in Intel Architecture (IA) based IoT platformsUnderstand the threat pyramid, secure boot, chain of trust, and the software stack leading up to defense-in-depth Who This Book Is For Strategists, developers, architects, and managers in the embedded and Internet of Things (IoT) space trying to understand and implement the security in the IoT devices/platforms.

Discusses Web browsing, cookies, anti-virus software, e-mail attachments, Web servers, public key infrastructure, secure remote access, virtual private networks, and cybercrime.

Securing Privacy in the Internet Age contains cutting-edge analyses of Internet privacy and security from some of the nation's leading legal practitioners and academics.