IoT Security Issues

Right here, we have countless ebook **IoT Security Issues** and collections to check out. We additionally give variant types and also type of the books to browse. The conventional book, fiction, history, novel, scientific research, as without difficulty as various extra sorts of books are readily nearby here.

As this IoT Security Issues , it ends up creature one of the favored books IoT Security Issues collections that we have. This is why you remain in the best website to see the amazing ebook to have.

Security of Internet of Things Nodes - Chinmay Chakraborty 2021-08-31
The book Security of Internet of Things Nodes: Challenges, Attacks, and Countermeasures® covers a wide range of research topics on the security of the Internet of Things nodes along with the latest research development in the domain of Internet of Things. It also covers various algorithms, techniques, and schemes in the field of computer science with state-of-the-art tools and technologies. This book mainly focuses on the security challenges of the Internet of Things devices and the countermeasures to overcome security vulnerabilities. Also, it highlights trust management issues on the Internet of Things nodes to build secured Internet of Things systems. The book also covers the necessity of a system model for the Internet of Things devices to ensure security at the hardware level.
Security, Privacy, and Forensics Issues in Big Data - Joshi, Ramesh C. 2019-08-30
With the proliferation of devices connected to the internet and connected to each other, the volume of data collected, stored, and processed is increasing every day, which brings new challenges in terms of information security. As big data expands with the help of public clouds, traditional security solutions tailored to private computing infrastructures and confined to a well-defined security perimeter, such as firewalls and demilitarized zones (DMZs), are no longer effective. New security functions are required to work over the heterogenous composition of diverse hardware, operating systems, and network domains. Security, Privacy, and Forensics Issues in Big Data is an essential research book that examines recent advancements in big data and the impact that these advancements have on information security and privacy measures needed for these networks. Highlighting a range of topics including cryptography, data analytics, and threat detection, this is an excellent reference source for students, software developers and engineers, security analysts, IT consultants, academicians, researchers, and professionals.
Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS) - Kuan-Ching Li 2020-12-16
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

Downloaded from test.unicaribe.edu.do on by guest

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.

Practical Internet of Things Security - Brian Russell 2016-06-29

A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world About This Book Learn to design and implement cyber security strategies for your organization Learn to protect cyber-physical systems and utilize forensic data analysis to beat vulnerabilities in your IoT ecosystem Learn best practices to secure your data from device to the cloud Gain insight into privacy-enhancing techniques and technologies Who This Book Is For This book targets IT Security Professionals and Security Engineers (including pentesters, security architects and ethical hackers) who would like to ensure security of their organization's data when connected through the IoT. Business analysts and managers will also find it useful. What You Will Learn Learn how to break down cross-industry barriers by adopting the best practices for IoT deployments Build a rock-solid security program for IoT that is cost-effective and easy to maintain Demystify complex topics such as cryptography, privacy, and penetration testing to improve your security posture See how the selection of individual components can affect the security posture of the entire system Use Systems Security Engineering and Privacy-by-design principles to design a secure IoT ecosystem Get to know how to leverage the burdgening cloud-based systems that will support the IoT into the future. In Detail With the advent of Intenret of Things (IoT), businesses will be faced with defending against new types of threats. The business ecosystem now includes cloud computing infrastructure, mobile and fixed endpoints that open up new attack surfaces, a desire to share information with many stakeholders and a need to take action quickly based on large quantities of collected data. . It therefore becomes critical to ensure that cyber security threats are contained to a minimum when implementing new IoT services and solutions. . The interconnectivity of people, devices, and companies raises stakes to a new level as computing and action become even more mobile, everything becomes connected to the cloud, and infrastructure is strained to securely manage the billions of devices that will connect us all to the IoT. This book shows you how to implement cyber-security solutions, IoT design best practices and risk mitigation methodologies to address device and infrastructure threats to IoT solutions. This book will take readers on a journey that begins with understanding the IoT and how it can be applied in various industries, goes on to describe the security challenges associated with the IoT, and then provides a set of guidelines to architect and deploy a secure IoT in your Enterprise. The book will showcase how the IoT is implemented in early-adopting industries and describe how lessons can be learned and shared across diverse industries to support a secure IoT. Style and approach This book aims to educate readers on key areas in IoT security. It walks readers through engaging with security challenges and then provides answers on how to successfully manage IoT security and build a safe infrastructure for smart devices. After reading this book, you will understand the true potential of tools and solutions in order to build real-time security intelligence on IoT networks.

Digital Cities Roadmap - Anand Nayyar 2021-03-29

DIGITAL CITIES ROADMAP This book details applications of technology to efficient digital city infrastructure and its planning, including smart buildings. Rapid urbanization, demographic changes, environmental changes, and new technologies are changing the views of urban leaders on sustainability, as well as creating and providing public services to tackle these new dynamics. Sustainable development is an objective by which the processes of planning, implementing projects, and development is aimed at meeting the needs of modern communities without compromising the potential

Downloaded from test.unicaribe.edu.do on by guest

of future generations. The advent of Smart Cities is the answer to these problems. Digital Cities Roadmap provides an in-depth analysis of design technologies that lay a solid foundation for sustainable buildings. The book also highlights smart automation technologies that help save energy, as well as various performance indicators needed to make construction easier. The book aims to create a strong research community, to have a deep understanding and the latest knowledge in the field of energy and comfort, to offer solid ideas in the nearby future for sustainable and resilient buildings. These buildings will help the city grow as a smart city. The smart city has also a focus on low energy consumption, renewable energy, and a small carbon footprint. Audience The information provided in this book will be of value to researchers, academicians and industry professionals interested in IoT-based architecture and sustainable buildings, energy efficiency and various tools and methods used to develop green technologies for construction in smart cities.

Internet of Things - S. Velliangiri 2020-12-30
IoT is empowered by various technologies used to detect, gather, store, act, process, transmit, oversee, and examine information. The combination of emergent technologies for information processing and distributed security, such as Cloud computing, Artificial intelligence, and Blockchain, brings new challenges in addressing distributed security methods that form the foundation of improved and eventually entirely new products and services. As systems interact with each other, it is essential to have an agreed interoperability standard, which is safe and valid. This book aims at providing an introduction by illustrating state-of-the-art security challenges and threats in IoT and the latest developments in IoT with Cloud, AI, and Blockchain security challenges. Various application case studies from domains such as science, engineering, and healthcare are introduced, along with their architecture and how they leverage various technologies Cloud, AI, and Blockchain. This book provides a comprehensive guide to researchers and students to design IoT integrated AI, Cloud, and Blockchain projects and to have an overview of the next generation challenges that may arise in the coming years.

Convergence of Deep Learning in Cyber-IoT Systems and Security - Rajdeep Chakraborty 2022-11-08
CONVERGENCE OF DEEP LEARNING IN CYBER-IOT SYSTEMS AND SECURITY In-depth analysis of Deep Learning-based cyber-IoT systems and security which will be the industry leader for the next ten years. The main goal of this book is to bring to the fore unconventional cryptographic methods to provide cyber security, including cyber-physical system security and IoT security through deep learning techniques and analytics with the study of all these systems. This book provides innovative solutions and implementation of deep learning-based models in cyber-IoT systems, as well as the exposed security issues in these systems. The 20 chapters are organized into four parts. Part I gives the various approaches that have evolved from machine learning to deep learning. Part II presents many innovative solutions, algorithms, models, and implementations based on deep learning. Part III covers security and safety aspects with deep learning. Part IV details cyber-physical systems as well as a discussion on the security and threats in cyber-physical systems with probable solutions. Audience Researchers and industry engineers in computer science, information technology, electronics and communication, cybersecurity and cryptography.

IoT Protocols and Applications for Improving Industry, Environment, and Society - Cristian González García 2021
"This book studies how daily life operates using many objects with Internet connections such as smartphones, tablets, Smart TVs, micro-controllers, Smart Tags, computers, laptops, cars, cheaper sensors, and more, commonly referred to as the Internet of Things. To accommodate this new connected structure, readers will learn how improved wireless strategies drive the need for a better IoT network"--

Security and Privacy Preserving for IoT and 5G Networks - Ahmed A. Abd El-Latif 2021-10-09
This book presents state-of-the-art research on security and privacy- preserving for IoT and 5G networks and applications. The accepted book chapters covered many themes, including

Downloaded from test.unicaribe.edu.do on by guest

traceability and tamper detection in IoT enabled waste management networks, secure Healthcare IoT Systems, data transfer accomplished by trustworthy nodes in cognitive radio, DDoS Attack Detection in Vehicular Ad-hoc Network (VANET) for 5G Networks, Mobile Edge-Cloud Computing, biometric authentication systems for IoT applications, and many other applications It aspires to provide a relevant reference for students, researchers, engineers, and professionals working in this particular area or those interested in grasping its diverse facets and exploring the latest advances on security and privacy- preserving for IoT and 5G networks.

Internet of Medical Things - D. Jude Hemanth 2021-04-13

This book looks at the growing segment of Internet of Things technology (IoT) known as Internet of Medical Things (IoMT), an automated system that aids in bridging the gap between isolated and rural communities and the critical healthcare services that are available in more populated and urban areas. Many technological aspects of IoMT are still being researched and developed, with the objective of minimizing the cost and improving the performance of the overall healthcare system. This book focuses on innovative IoMT methods and solutions being developed for use in the application of healthcare services, including post-surgery care, virtual home assistance, smart real-time patient monitoring, implantable sensors and cameras, and diagnosis and treatment planning. It also examines critical issues around the technology, such as security vulnerabilities, IoMT machine learning approaches, and medical data compression for lossless data transmission and archiving. Internet of Medical Things is a valuable reference for researchers, students, and postgraduates working in biomedical, electronics, and communications engineering, as well as practicing healthcare professionals.

Computer Science and its Applications - James J. Jong Hyuk Park 2014-12-15

The 6th FTRA International Conference on Computer Science and its Applications (CSA-14) will be held in Guam, USA, Dec. 17 - 19, 2014. CSA-14 presents a comprehensive conference focused on the various aspects of advances in engineering systems in computer science, and applications, including ubiquitous computing, U-Health care system, Big Data, UI/UX for human-centric computing, Computing Service, Bioinformatics and Bio-Inspired Computing and will show recent advances on various aspects of computing technology, Ubiquitous Computing Services and its application.

Research Anthology on Privatizing and Securing Data - Management Association, Information Resources 2021-04-23

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.

Security and Privacy in the Internet of Things - Ali Ismail Awad 2021-12-29

SECURITY AND PRIVACY IN THE INTERNET OF THINGS Provides the authoritative and up-to-date information required for securing IoT

Downloaded from test.unicaribe.edu.do on by guest

architecture and applications The vast amount of data generated by the Internet of Things (IoT) has made information and cyber 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 security models, architectures, techniques, and application domains. This concise yet comprehensive volume explores state-of-the-art mitigations in IoT security while addressing important security and privacy challenges across different IoT layers. 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 environments and e-health. Topics include authentication and access control, attack detection and prevention, securing IoT through traffic modeling, human aspects in IoT security, and IoT hardware security. Presenting the current body of knowledge in a single volume, Security and Privacy in the Internet of Things: Discusses a broad range of IoT attacks and defense mechanisms Examines IoT security and privacy protocols and approaches Covers both the logical and physical security of IoT devices Addresses IoT security through network traffic modeling Describes privacy preserving techniques in smart cities Explores current 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 security development and IoT systems deployment.

Security and Privacy Issues in Sensor Networks and IoT - Ahlawat, Priyanka 2019-10-25

As technology continues to expand and develop, the internet of things (IoT) is playing a progressive role in the infrastructure of electronics. The increasing amount of IoT devices, however, has led to the emergence of significant privacy and security challenges. Security and Privacy Issues in Sensor Networks and IoT is a collection of innovative research on the methods and applications of protection disputes in the internet of things and other computing structures. While highlighting topics that include cyber defense, digital forensics, and intrusion detection, this book is ideally designed for security analysts, IT specialists, software developers, computer engineers, industry professionals, academicians, students, and researchers seeking current research on defense concerns in cyber physical systems.

Integrating AI in IoT Analytics on the Cloud for Healthcare Applications - Jeya Mala, D. 2022-01-07

Internet of things (IoT) applications employed for healthcare generate a huge amount of data that needs to be analyzed to produce the expected reports. To accomplish this task, a cloud-based analytical solution is ideal in order to generate faster reports in comparison to the traditional way. Given the current state of the world in which every day IoT devices are developed to provide healthcare solutions, it is essential to consider the mechanisms used to collect and analyze the data to provide thorough reports. Integrating AI in IoT Analytics on the Cloud for Healthcare Applications applies artificial intelligence (AI) in edge analytics for healthcare applications, analyzes the impact of tools and techniques in edge analytics for healthcare, and discusses security solutions for edge analytics in healthcare IoT. Covering topics such as data analytics and next generation healthcare systems, it is ideal for researchers, academicians, technologists, IT specialists, data scientists, healthcare industries, IoT developers, data security analysts, educators, and students.

Internet of Things Security: Principles and Practice - Qinghao Tang 2021-01-27

Over the past few years, Internet of Things has brought great changes to the world. Reports show that, the number of IoT devices is expected to reach 10 billion units within the next three years. The number will continue to rise and wildly use as infrastructure and housewares with each passing day, Therefore, ensuring the safe and stable operation of IoT devices has become more important for IoT manufacturers. Generally, four key aspects are involved in security risks when users use typical IoT products such as routers, smart speakers, and in-car entertainment systems, which are cloud, terminal, mobile device applications, and communication data. Security issues concerning any of the four may lead to the leakage of user

Downloaded from test.unicaribe.edu.do on by guest

sensitive data. Another problem is that most IoT devices are upgraded less frequently, which leads it is difficult to resolve legacy security risks in short term. In order to cope with such complex security risks,Security Companies in China, such as Qihoo 360, Xiaomi, Alibaba and Tencent, and companies in United States, e.g. Amazon, Google, Microsoft and some other companies have invested in security teams to conduct research and analyses, the findings they shared let the public become more aware of IoT device security-related risks. Currently, many IoT product suppliers have begun hiring equipment evaluation services and purchasing security protection products. As a direct participant in the IoT ecological security research project, I would like to introduce the book to anyone who is a beginner that is willing to start the IoT journey, practitioners in the IoT ecosystem, and practitioners in the security industry. This book provides beginners with key theories and methods for IoT device penetration testing; explains various tools and techniques for hardware, firmware and wireless protocol analysis; and explains how to design a secure IoT device system, while providing relevant code details.

IoT Applications, Security Threats, and Countermeasures - Padmalaya Nayak 2021

"The book explores modern sensor technologies while also discussing security issues, which is the dominant factor for many types of Internet of Things (IoT) applications. It also covers recent (IoT) applications such as the Markovian Arrival Process, fog computing, real-time solar energy monitoring, healthcare, and agriculture. Fundamental concepts of gathering, processing, and analyzing different Artificial Intelligence (AI) models in IoT applications are covered along with recent detection mechanisms for different types of attacks for effective network communication. On par with the standards laid out by international organizations in related fields, the book focuses on both core concepts of IoT along with major application areas. Designed for technical developers, academicians, data scientists, industrial researchers, professionals, and students, this book is useful in uncovering the latest innovations in the field of IoT"--

Advanced Security Issues of IoT Based 5G Plus Wireless Communication for Industry 4. 0 - Vijey Thayananthan, Ph.d. 2019-05-17

Advanced IoT based wireless communication has recently received a lot of attention due to a wide range of industry 4.0 applications such as security solutions of CPS in vehicular communication, E_Healthcare over secure wireless communication, privacy issues of E_Learning via cost and energy efficient wireless network communication, etc. In these applications, physical data is continuously monitored by the IoT-based sensor nodes to facilitate the current situations, 5G network management, security solutions, etc. in industry 4.0 environment. Despite the many security issues considered in existing wireless communication in the industry 4.0 applications, IoT based 5G and 5G+ wireless communication will enhance the future security issues including cybersecurity solutions. The aim of this book to deliver the best services with minimum cost and maximum security in all industry 4.0 applications. For instance, medical priority services against the available sources and devices (IoT, sensors, decision-making units, etc.), patient monitoring services against the waiting list and the population, and security services of CPS against the energy efficiency and the battery lifetime are challenging critical problems in the industry 4.0. This book covers some improvement methods in security influence to future communication they are cybersecurity issues of IoT based 5G and 5G+ communication systems. These methods can be considered through the efficient channel coding scheme, efficient traffic management, bandwidth guard, cybersecurity solutions, etc. Requirements for future communication such 5G+ support to illustrate the security issues in selected applications of industry 4.0 such as learning style transformation. Sensors are typically capable of wireless communication and are significantly utilized in many applications such as medical communication with IoT-based 5G infrastructure. Despite many security solutions of communication technologies, decision making, dynamic and intelligent solutions based on sensors, IoT devices, CPS, etc. will be minimizing energy costs and maximizing security issues of industry 4.0. The field of advanced IoT-based 5G+ wireless communication networks merge a lot of

Downloaded from test.unicaribe.edu.do on by guest

functions like secure transmission capacities with latest multiple access schemes, computation of best latency and energy efficiency, and secure communication with location-based services, etc. This book covers many functionalities through the important examples and applications used in industry 4.0.

Security and Organization Within IoT and Smart Cities - Kayhan Zrar Ghafoor 2020-12-31

This book aims to provide the latest research developments and results in the domain of AI techniques for smart cyber ecosystems. It presents a holistic insight into AI-enabled theoretic approaches and methodology in IoT networking, security analytics using AI tools and network automation, which ultimately enable intelligent cyber space. This book will be a valuable resource for students, researchers, engineers and policy makers working in various areas related to cybersecurity and privacy for Smart Cities. This book includes chapters titled "An Overview of the Artificial Intelligence Evolution and Its Fundamental Concepts, and Their Relationship with IoT Security", "Smart City: Evolution and Fundamental Concepts", "Advances in AI-Based Security for Internet of Things in Wireless Virtualization Environment", "A Conceptual Model for Optimal Resource Sharing of Networked Microgrids Focusing Uncertainty: Paving Path to Eco-friendly Smart Cities", "A Novel Framework for a Cyber Secure Smart City", "Contemplating Security Challenges and Threats for Smart Cities", "Self-Monitoring Obfuscated IoT Network", "Introduction to Side Channel Attacks and Investigation of Power Analysis and Fault Injection Attack Techniques", "Collaborative Digital Forensic Investigations Model for Law Enforcement: Oman as a Case Study", "Understanding Security Requirements and Challenges in the Industrial Internet of Things: A Review", "5G Security and the Internet of Things", "The Problem of Deepfake Videos and How to Counteract Them in Smart Cities", "The Rise of Ransomware Aided by Vulnerable IoT Devices", "Security Issues in Self-Driving Cars within Smart Cities", and "Trust-Aware Crowd Associated Network-Based Approach for Optimal Waste Management in Smart Cities". This book provides state-of-the-art research results and discusses current issues, challenges, solutions and recent trends related to security and organization within IoT and Smart Cities. We expect this book to be of significant importance not only to researchers and practitioners in academia, government agencies and industries, but also for policy makers and system managers. We anticipate this book to be a valuable resource for all those working in this new and exciting area, and a "must have" for all university libraries.

Practical IoT Hacking - Fotios Chantzis 2021-03-23

The definitive guide to hacking the world of the Internet of Things (IoT) -- Internet connected devices such as medical devices, home assistants, smart home appliances and more. Drawing from the real-life exploits of five highly regarded IoT security researchers, Practical IoT Hacking teaches you how to test IoT systems, devices, and protocols to mitigate risk. The book begins by walking you through common threats and a threat modeling framework. You'll develop a security testing methodology, discover the art of passive reconnaissance, and assess security on all layers of an IoT system. Next, you'll perform VLAN hopping, crack MQTT authentication, abuse UPnP, develop an mDNS poisoner, and craft WS-Discovery attacks. You'll tackle both hardware hacking and radio hacking, with in-depth coverage of attacks against embedded IoT devices and RFID systems. You'll also learn how to: • Write a DICOM service scanner as an NSE module • Hack a microcontroller through the UART and SWD interfaces • Reverse engineer firmware and analyze mobile companion apps • Develop an NFC fuzzer using Proxmark3 • Hack a smart home by jamming wireless alarms, playing back IP camera feeds, and controlling a smart treadmill The tools and devices you'll use are affordable and readily available, so you can easily practice what you learn. Whether you're a security researcher, IT team member, or hacking hobbyist, you'll find Practical IoT Hacking indispensable in your efforts to hack all the things REQUIREMENTS: Basic knowledge of Linux command line, TCP/IP, and programming

Interoperability in IoT for Smart Systems - Monideepa Roy 2020-12-17

Interoperability in IoT for Smart Systems discusses the different facets of interoperability issues among the IoT devices and their solutions,

Downloaded from test.unicaribe.edu.do on by guest

the scalability issues in an IoT network, and provides solutions for plug-n-play of new devices with the existing IoT system. It also addresses the possible usage of interoperable and plug-n-play IoT networks in different systems to make them smarter. Aimed at researchers and graduate students in computer science, computer engineering, computer networks, electronics engineering, this book Exclusively covers interoperability of IoT systems in parallel with their use towards the development of smart systems Discusses the requirements of interoperability in smart IoT systems and their solutions Reviews IoT applications in different smart and intelligent systems Explores dealing with interoperability of heterogeneous participating devices Provides different case studies and open problems related to interoperability in IoT systems

Cyber Threat Intelligence for the Internet of Things - Elias Bou-Harb 2020-05-30

This book reviews IoT-centric vulnerabilities from a multidimensional perspective by elaborating on IoT attack vectors, their impacts on well-known security objectives, attacks which exploit such vulnerabilities, coupled with their corresponding remediation methodologies. This book further highlights the severity of the IoT problem at large, through disclosing incidents of Internet-scale IoT exploitations, while putting forward a preliminary prototype and associated results to aid in the IoT mitigation objective. Moreover, this book summarizes and discloses findings, inferences, and open challenges to inspire future research addressing theoretical and empirical aspects related to the imperative topic of IoT security. At least 20 billion devices will be connected to the Internet in the next few years. Many of these devices transmit critical and sensitive system and personal data in real-time. Collectively known as “the Internet of Things” (IoT), this market represents a $267 billion per year industry. As valuable as this market is, security spending on the sector barely breaks 1%. Indeed, while IoT vendors continue to push more IoT devices to market, the security of these devices has often fallen in priority, making them easier to exploit. This drastically threatens the privacy of the consumers and the safety of mission-critical systems. This book is intended for cybersecurity researchers and advanced-level students in computer science. Developers and operators working in this field, who are eager to comprehend the vulnerabilities of the Internet of Things (IoT) paradigm and understand the severity of accompanied security issues will also be interested in this book.

IoT Security Issues - Alasdair Gilchrist 2017-01-23

IoT Security Issues looks at the burgeoning growth of devices of all kinds controlled over the Internet of all varieties, where product comes first and security second. In this case, security trails badly. This book examines the issues surrounding these problems, vulnerabilities, what can be done to solve the problem, investigating the stack for the roots of the problems and how programming and attention to good security practice can combat the problems today that are a result of lax security processes on the Internet of Things. This book is for people interested in understanding the vulnerabilities on the Internet of Things, such as programmers who have not yet been focusing on the IoT, security professionals and a wide array of interested hackers and makers. This book assumes little experience or knowledge of the Internet of Things. To fully appreciate the book, limited programming background would be helpful for some of the chapters later in the book, though the basic content is explained. The author, Alasdair Gilchrist, has spent 25 years as a company director in the fields of IT, Data Communications, Mobile Telecoms and latterly Cloud/SDN/NFV technologies, as a professional technician, support manager, network and security architect. He has project-managed both agile SDLC software development as well as technical network architecture design. He has experience in the deployment and integration of systems in enterprise, cloud, fixed/mobile telecoms, and service provider networks. He is therefore knowledgeable in a wide range of technologies and has written a number of books in related fields.

Agricultural Informatics - Amitava Choudhury 2021-03-02

Despite the increasing population (the Food and Agriculture Organization of the United Nations estimates 70% more food will be needed in 2050 than was produced in 2006), issues related to food production have yet to be completely

Downloaded from test.unicaribe.edu.do on by guest

addressed. In recent years, Internet of Things technology has begun to be used to address different industrial and technical challenges to meet this growing need. These Agro-IoT tools boost productivity and minimize the pitfalls of traditional farming, which is the backbone of the world's economy. Aided by the IoT, continuous monitoring of fields provides useful and critical information to farmers, ushering in a new era in farming. The IoT can be used as a tool to combat climate change through greenhouse automation; monitor and manage water, soil and crops; increase productivity; control insecticides/pesticides; detect plant diseases; increase the rate of crop sales; cattle monitoring etc. Agricultural Informatics: Automation Using the IoT and Machine Learning focuses on all these topics, including a few case studies, and they give a clear indication as to why these techniques should now be widely adopted by the agriculture and farming industries.

Blockchain Applications in IoT Security - Patel, Harshita 2020-09-18

Like many other scientific innovations, scientists are looking to protect the internet of things (IoT) from unfortunate losses, theft, or misuse. As one of the current hot trends in the digital world, blockchain technology could be the solution for securing the IoT. Blockchain Applications in IoT Security presents research for understanding IoT-generated data security issues, existing security facilities and their limitations and future possibilities, and the role of blockchain technology. Featuring coverage on a broad range of topics such as cryptocurrency, remote monitoring, and smart computing, this book is ideally designed for security analysts, IT specialists, entrepreneurs, business professionals, academicians, researchers, students, and industry professionals seeking current studies on the limitations and possibilities behind competitive blockchain technologies.

Securing the Internet of Things - Shancang Li 2017-01-11

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

Handbook of e-Business Security - João Manuel R.S. Tavares 2018-07-27

There are a lot of e-business security concerns. Knowing about e-business security issues will likely help overcome them. Keep in mind, companies that have control over their e-business are likely to prosper most. In other words, setting up and maintaining a secure e-business is essential and important to business growth. This book covers state-of-the art practices in e-business security, including privacy, trust, security of transactions, big data, cloud computing, social network, and distributed systems.

Security and Privacy Issues in IoT Devices and Sensor Networks - Sudhir Kumar Sharma 2020-10-15

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

Downloaded from test.unicaribe.edu.do on by guest

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

Deep Learning Approaches for Security Threats in IoT Environments - Mohamed Abdel-Basset 2022-12-20

Deep Learning Approaches for Security Threats in IoT Environments An expert discussion of the application of deep learning methods in the IoT security environment In Deep Learning Approaches for Security Threats in IoT Environments, a team of distinguished cybersecurity educators deliver an insightful and robust exploration of how to approach and measure the security of Internet-of-Things (IoT) systems and networks. In this book, readers will examine critical concepts in artificial intelligence (AI) and IoT, and apply effective strategies to help secure and protect IoT networks. The authors discuss supervised, semi-supervised, and unsupervised deep learning techniques, as well as reinforcement and federated learning methods for privacy preservation. This book applies deep learning approaches to IoT networks and solves the security problems that professionals frequently encounter when working in the field of IoT, as well as providing ways in which smart devices can solve cybersecurity issues. Readers will also get access to a companion website with PowerPoint presentations, links to supporting videos, and additional resources. They'll also find: A thorough introduction to artificial intelligence and the Internet of Things, including key concepts like deep learning, security, and privacy Comprehensive discussions of the architectures, protocols, and standards that form the foundation of deep learning for securing modern IoT systems and networks In-depth examinations of the architectural design of cloud, fog, and edge computing networks Fulsome presentations of the security requirements, threats, and countermeasures relevant to IoT networks Perfect for professionals working in the AI, cybersecurity, and IoT industries, Deep Learning Approaches for Security Threats in IoT Environments will also earn a place in the libraries of undergraduate and graduate students studying deep learning, cybersecurity, privacy preservation, and the security of IoT networks.

Demystifying Internet of Things Security - Sunil Cheruvu 2019-08-13

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.

Security Issues and Privacy Threats in Smart Ubiquitous Computing - Parikshit N. Mahalle 2021-04-08

Downloaded from test.unicaribe.edu.do on by guest

This book extends the work from introduction of ubiquitous computing, to the Internet of things to security and to privacy aspects of ubiquitous computing. The uniqueness of this book is the combination of important fields like the Internet of things and ubiquitous computing. It assumes that the readers' goal is to achieve a complete understanding of IoT, smart computing, security issues, challenges and possible solutions. It is not oriented towards any specific use cases and security issues; privacy threats in ubiquitous computing problems are discussed across various domains. This book is motivating to address privacy threats in new inventions for a wide range of stakeholders like layman to educated users, villages to metros and national to global levels. This book contains numerous examples, case studies, technical descriptions, scenarios, procedures, algorithms and protocols. The main endeavour of this book is threat analysis and activity modelling of attacks in order to give an actual view of the ubiquitous computing applications. The unique approach will help readers for a better understanding.

Examining Cloud Computing Technologies Through the Internet of Things - Tomar, Pradeep 2017-11-30

The progressive combination of cloud computing and Internet of Things (IoT) will enable new monitoring services, create powerful processing of sensory data streams, and provide a new method for intelligent perception and connection. Examining Cloud Computing Technologies Through the Internet of Things is a pivotal reference source for scholarly research on the latest and innovative facets of cloud-based Internet of Things systems including technical evaluations and comparisons of existing concepts. Featuring coverage on a broad range of topics such as fog computing, network programming, and data security, this book is geared towards advanced-level students, researchers, and professionals interested in exploring and implementing the IoT and related technologies.

Privacy Vulnerabilities and Data Security Challenges in the Iot - Shivani Agarwal 2020-10

Privacy Vulnerabilities and Data Security Challenges in the IoT Subject Guide: Engineering--Industrial and Manufacturing This book discusses the evolution of security and privacy issues in the Internet of Things (IoT). The book focuses on assembling all security- and privacy-related technologies into a single source so that students, researchers, academics, and those in the industry can easily understand the IoT security and privacy issues. This edited book discusses the use of 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 security issues in IoT-enabled technologies and how these can be applied in various sectors. It walks readers through engaging with security challenges and building a safe infrastructure for IoT devices. The book helps researchers and practitioners understand the security architecture of IoT and the state-of-the-art in 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 and WSNs in IoT. This book aims to highlight the concepts of related technologies and novel findings by researchers through its chapter organization. The primary audience comprises specialists, researchers, graduate students, designers, experts, and engineers undertaking research on security-related issues.

Security and Privacy in Internet of Things (Iots) - Fei Hu 2020-06-30

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

Downloaded from test.unicaribe.edu.do on by guest

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 IoT.

Security Issues and Privacy Concerns in Industry 4.0 Applications - Shibin David 2021-08-24

SECURITY ISSUES AND PRIVACY CONCERNS IN INDUSTRY 4.0 APPLICATIONS Written and edited by a team of international experts, this is the most comprehensive and up-to-date coverage of the security and privacy issues surrounding Industry 4.0 applications, a must-have for any library. The scope of Security Issues and Privacy Concerns in Industry 4.0 Applications is to envision the need for security in Industry 4.0 applications and the research opportunities for the future. This book discusses the security issues in Industry 4.0 applications for research development. It will also enable the reader to develop solutions for the security threats and attacks that prevail in the industry. The chapters will be framed on par with advancements in the industry in the area of Industry 4.0 with its applications in additive manufacturing, cloud computing, IoT (Internet of Things), and many others. This book helps a researcher and an industrial specialist to reflect on the latest trends and the need for technological change in Industry 4.0. Smart water management using IoT, cloud security issues with network forensics, regional language recognition for industry 4.0, IoT-based health care management systems, artificial intelligence for fake profile detection, and packet drop detection in agriculture-based IoT are covered in this outstanding new volume. Leading innovations such as smart drone for railway track cleaning, everyday life-supporting blockchain and big data, effective prediction using machine learning, classification of dog breed based on CNN, load balancing using the SPE approach and cyber culture impact on media consumers are also addressed. Whether a reference for the veteran engineer or an introduction to the technologies covered in the book for the student, this is a must-have for any library.

Security in IoT-Enabled Spaces - Fadi Al-Turjman 2019-02-07

Security and smart spaces are among the most significant topics in IoT nowadays. The implementation of secured smart spaces is at the heart of this concept, and its development is a key issue in the next generation IoT. This book addresses major security aspects and challenges in realizing smart spaces and sensing platforms in critical Cloud and IoT applications. The book focuses on both the design and implementation aspects of security models and strategies in smart that are enabled by wireless sensor networks and RFID systems. It mainly examines seamless data access approaches and encryption and decryption aspects in reliable IoT systems.

Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems - Geetha, S. 2019-02-22

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

Downloaded from test.unicaribe.edu.do on by guest

investigations, standards, and policies. It is designed for policymakers, forensic analysts, technology developers, security administrators, academicians, researchers, and students.

IoT Security - Madhusanka Liyanage 2019-12-02

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

Security Breaches and Threat Prevention in the Internet of Things - Jeyanthi, N. 2017-02-01

As the applications of the Internet of Things continue to progress, so do the security concerns for this technology. The study of threat prevention in the Internet of Things is necessary, as security breaches in this field can ruin industries and lives. Security Breaches and Threat Prevention in the Internet of Things provides a comprehensive examination of the latest strategies and methods for tracking and blocking threats within industries that work heavily with this technology. Featuring chapters on emerging topics such as security threats in autonomous vehicles, digital forensics, secure communications, and image encryption, this critical reference source is a valuable tool for all academicians, graduate students, practitioners, professionals, and researchers who are interested in expanding their knowledge of security practices pertaining to the Internet of Things.

IoT - Souvik Pal 2020-06-03

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 understand 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,

Downloaded from test.unicaribe.edu.do on by guest

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.

Downloaded from test.unicaribe.edu.do on by guest