Security and Privacy Preserving for IoT and 5G Networks

The book aims to integrate the aspects of IoT, Cloud computing and data analytics from diversified perspectives. The book also plans to discuss the recent research trends and advanced topics in the field which will be of interest to academicians and researchers working in this area. Thus, the book intends to help its readers to understand and explore the spectrum of applications of IoT, cloud computing and data analytics. Here, it is also worth mentioning that the book is believed to draw attention on the applications of said technology in various disciplines in order to obtain enhanced understanding of the readers. Also, this book focuses on the researches and challenges in the domain of IoT, Cloud computing and Data analytics from perspectives of various stakeholders.

Securing the Internet of Things

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

**Security and Privacy Issues in IoT Devices and Sensor Networks**

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.

**Transforming Businesses With Bitcoin Mining and Blockchain Applications**

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 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.

**Computer Science and its Applications**

"This book focuses on the security, privacy, and forensics of big data. It also examines the principles, algorithms, challenges and applications related to the security, privacy, and forensics of big data"--

**Digital Cities Roadmap**

The ubiquity of modern technologies has allowed for increased connectivity between people and devices across the globe. This connected infrastructure of networks creates numerous opportunities for applications and uses. 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. Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications is a vital reference source that examines recent developments and emerging trends in security and privacy for the internet of things through new models, practical solutions, and technological advancements related to security. Highlighting a range of topics such as cloud security, threat detection, and open source software, this multi-volume book is ideally designed for engineers, IT consultants, ICT procurement managers, network system integrators, infrastructure service providers, researchers, academics, and professionals interested in current research on security practices pertaining to the internet of things.

**Security Challenges and Approaches in Internet of Things**

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 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.

**Quantum Cryptography and the Future of Cyber Security**

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.

Privacy Vulnerabilities and Data Security Challenges in the IoT

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 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.

Security and Organization within IoT and Smart Cities

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.

IoT Applications, Security Threats, and Countermeasures

This book provides a comprehensive survey of the security and privacy research advancements in Internet of Things (IoT). The book lays the context for the discussion by introducing a system model for IoT. Since IoT is very varied and has been introduced in many different contexts, the system model introduced plays a crucial role in integrating the concepts into a coherent framework. After the system model, the book introduces the vulnerable features of the IoT. By providing a comprehensive discussion of the vulnerable features, the book highlights the problem areas of IoT that should be studied concerning security and privacy. Using the vulnerable features as a motivation, the book presents a vast survey of existing security and privacy approaches for IoT. The survey is a good way for the reader to pick up interesting directions of research that have already been explored and also hints at directions that could take additional investigation. Finally, the book presents four case studies that provide a detailed view of how some of the security and privacy concerns are addressed in specific problem areas.
Digital Twin Technologies and Smart Cities

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.

Internet of Things

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.

Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications

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.

**IoT Applications, Security Threats, and Countermeasures**

This book provides a comprehensive survey of the security and privacy research advancements in Internet of Things (IoT). The book lays the context for the discussion by introducing a system model for IoT. Since IoT is very varied and has been introduced in many different contexts, the system model introduced plays a crucial role in integrating the concepts into a coherent framework. After the system model, the book introduces the vulnerable features of the IoT. By providing a comprehensive discussion of the vulnerable features, the book highlights the problem areas of IoT that should be studied concerning security and privacy. Using the vulnerable features as a motivation, the book presents a vast survey of existing security and privacy approaches for IoT. The survey is a good way for the reader to pick up interesting directions of research that have already been explored and also hints at directions that could take additional investigation. Finally, the book presents four case studies that provide a detailed view of how some of the security and privacy concerns are addressed in specific problem areas.

**2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)**

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.

**Internet of Things Security**

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.

**Internet of Things Security**

"This book studies how daily life operates using many objects with Internet connections such as smartphones, tablets, Smart TVs, micro-controllable, 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 Issues in Sensor Networks and IoT**

Managing the Web of Things: Linking the Real World to the Web presents a consolidated and holistic coverage of engineering, management, and analytics of the Internet of Things. The web has gone through many transformations, from traditional linking and sharing of computers and documents (i.e., Web of Data), to the current connection of people (i.e., Web of People), and to the emerging connection of billions of physical objects (i.e., Web of Things). With increasing numbers of electronic devices and systems providing different services to people, Web of Things applications present numerous challenges to research institutions, companies, governments, international organizations, and others. This book compiles the newest developments and advances in the area of the Web of Things, ranging from modeling, searching, and data analytics, to software building, applications, and social impact. Its coverage will enable effective exploration, understanding, assessment, comparison, and the selection of WoT models, languages, techniques, platforms, and tools. Readers will gain an up-to-date understanding of the Web of Things systems that accelerates their research. Offers a comprehensive and systematic presentation of the methodologies, technologies, and applications that enable efficient and effective management of the Internet of Things Provides an in-depth analysis on the state-of-the-art Web of Things modeling and searching technologies, including how to collect, clean, and analyze data generated by the Web of Things Covers system design and software building principles, with discussions and explorations of social impact for the Web of Things through real-world applications Acts as an ideal reference or recommended text for graduate courses in cloud computing, service computing, and more

**Security of Internet of Things Nodes**
This book provides a holistic perspective on Digital Twin (DT) technologies, and presents cutting-edge research in the field. It assesses the opportunities that DT can offer for smart cities, and covers the requirements for ensuring secure, safe and sustainable smart cities. Further, the book demonstrates that DT and its benefits with regard to: data visualisation, real-time data analytics, and learning leading to improved confidence in decision making; reasoning, monitoring and warning to support accurate diagnostics and prognostics; acting using edge control and what-if analysis; and connection with back-end business applications hold significant potential for applications in smart cities, by employing a wide range of sensory and data-acquisition systems in various parts of the urban infrastructure. The contributing authors reveal how and why DT technologies that are used for monitoring, visualising, diagnosing and predicting in real-time are vital to cities' sustainability and efficiency. The concepts outlined in the book represents a city together with all of its infrastructure elements, which communicate with each other in a complex manner. Moreover, securing Internet of Things (IoT) which is one of the key enablers of DT’s is discussed in details and from various perspectives. The book offers an outstanding reference guide for practitioners and researchers in manufacturing, operations research and communications, who are considering digitising some of their assets and related services. It is also a valuable asset for graduate students and academics who are looking to identify research gaps and develop their own proposals for further research.

### Securing the Internet of Things

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 an overview of different security solutions What You'll Learn how to Secure devices, immunizing them against different threats originating from inside and outside the network.Gather 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.

### Integration of Cloud Computing with Internet of Things

The shortcomings of modern cryptography and its weaknesses against computers that are becoming more powerful necessitate serious consideration of more robust security options. Quantum cryptography is sound, and its practical implementations are becoming more mature. Many applications can use quantum cryptography as a backbone, including key distribution, secure direct communications, large prime factorization, e-commerce, e-governance, quantum internet, and more. For this reason, quantum cryptography is gaining interest and importance among computer and security professionals.
Quantum Cryptography and the Future of Cyber Security is an essential scholarly resource that provides the latest research and advancements in cryptography and cyber security through quantum applications. Highlighting a wide range of topics such as e-commerce, machine learning, and privacy, this book is ideal for security analysts, systems engineers, software security engineers, data scientists, vulnerability analysts, professionals, academicians, researchers, security professionals, policymakers, and students.

**Security Issues and Privacy Threats in Smart Ubiquitous Computing**

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

**Security, Privacy, and Forensics Issues in Big Data**

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.

**Security and Privacy in the Internet of Things**

"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..."
Access Free IoT Security Issues

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”--

IoT

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.

Managing the Web of Things

2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT 2019) will be held at University of Bahrain, Kingdom of Bahrain, September 22 23, 2019 The aim of 3ICT 2019 is to provide a forum for the researchers and industry practitioners to exchange the latest fundamental advances in the state of the art and practice of Computing, Advanced Technologies, and Invocative Research present their latest research results and perspectives for future work in these areas of research

Handbook of e-Business Security

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.

IoT Security

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, 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

This book provides state-of-the-art of 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.

Security and Privacy in Internet of Things (IoTs)

The success of many companies through the assistance of bitcoin proves that technology continually dominates and transforms how economics operate. However, a deeper, more conceptual understanding of how these technologies work to identify innovation opportunities and how to successfully thrive in an increasingly competitive environment is needed for the entrepreneurs of tomorrow. Transforming Businesses With Bitcoin Mining and Blockchain Applications provides innovative insights into IT infrastructure and emerging trends in the realm of digital business technologies. This publication analyzes and extracts information from Bitcoin networks and provides the necessary steps to designing open blockchain. Highlighting topics that include financial markets, risk management, and smart technologies, the research contained within the title is ideal for entrepreneurs, business professionals, managers, executives, academicians, researchers, and business students.

Demystifying Internet of Things Security

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.
Security Challenges and Approaches in Internet of Things

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.

Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS)

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.

Cyber Threat Intelligence for the Internet of Things

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.
Advanced Security Issues of IoT Based 5G Plus Wireless Communication for Industry 4.0

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.

Security Breaches and Threat Prevention in the Internet of Things

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 REQUISITE: Basic knowledge of Linux command line, TCP/IP, and programming

Blockchain Applications in IoT Security

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 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.

Iot Security Issues

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 Protocols and Applications for Improving Industry, Environment, and Society

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.
Things devices to ensure security at the hardware level.

**Practical IoT Hacking**

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.

Copyright code: 091f3948ea9092b992fbd54199dbc4e2