

Enhancing IoT Security

*A holistic approach to security for
connected platforms*

**Vidushi Sharma
Gamini Joshi**



www.bpbonline.com

Copyright © 2024 BPB Online

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor BPB Online or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

BPB Online has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, BPB Online cannot guarantee the accuracy of this information.

First published: 2024

Published by BPB Online

WeWork

119 Marylebone Road

London NW1 5PU

UK | UAE | INDIA | SINGAPORE

ISBN 978-93-55515-506

www.bpbonline.com

Dedicated to

Lord Shiva and Guru Sai – My Torch Bearer

*My Son **Shouryaa** for supporting me and
driving me to achieve my goals*

*My Husband **Rohit** and my Brother **Sadashiv** – My pillars of strength
– Dr. Vidushi Sharma*

My beloved:

*Parents: **Mr. Lalit Mohan Joshi** and **Mrs. Geeta Joshi***

*(For their endless love, support and encouragement
to achieve everything in life)*

&

*Parents-in-law: **Dr. S.P. Lohani** and **Mrs. Hema Lohani***

(For their continuous emotional and moral support)

&

*My Husband: **Mani Lohani***

*(For his continuous encouragement to improve my
knowledge and move ahead in my career)*

&

*My Daughter: **Mishthi Lohani***

*(For her smile that inspires me to always be
positive and give my best)*

– Gamini Joshi

About the Authors

- ❖ **Dr. Vidushi Sharma** has received the Ph.D. degree in computer science from Dr. B.R. Ambedkar University, Agra, India, in 2008. She is currently the Head of the Department of Electronics and Communication Engineering, and the Convenor of Centre of Rapid and Alternative Energy Mobility at Gautam Buddha University, Greater Noida, India. She teaches Doctoral, Postgraduate, and Graduate courses; and has authored over 100 research papers for international and national publications. She has also authored a book titled *Energy Efficient Wireless Sensor Network* (2017, Taylor and Francis). She has supervised nine Ph.D. students and more than 50 Dissertation students in the area of wireless sensor networks and the Internet of Things; mentored two - Department of Science and Technology, India projects. She also has two patents awarded and three patents published. Her research interests include IT applications and performance evaluation of information systems, which includes wireless sensor networks, Internet of Things. She has organized several conferences, workshops, and FDP and is also a reviewer for reputed journals.

- ❖ **Gamini Joshi** is pursuing Ph.D. at Gautam Buddha University, Greater Noida, India. She has worked as an assistant professor and has taught graduate-level courses. She has authored as well as co-authored a large number of papers for international and national publications. Her research interests include IT applications, performance evaluation, and security of IoT information systems, which include wireless sensor networks and the Internet of Things.

About the Reviewer

Anuj Gargeya Malkapuram is an accomplished Security Practitioner known for his leadership in cross-functional teams and enterprise-level security initiatives. With expertise in security detection, incident response, threat intelligence, and security engineering, Anuj evangelizes information security within organizations and beyond. He currently serves as a Principal Security Engineer at Salesforce and has previously worked at reputable companies like Amazon and LendingClub Corporation in FinTech, E-Commerce, and SaaS sectors. Anuj's contributions extend beyond the corporate realm, as he has filed multiple patents and published his work in international journals. He actively collaborates with non-profit organizations such as World Economic Forum, CENSA, and other recognized internet security entities. Anuj holds a Master's degree in Electrical Engineering, specializing in Computer Networking and Security, from San Jose State University.

Acknowledgements

- ❖ I want to express my deepest gratitude to the Almighty lord for holding my hand and guiding me on the path destined by him. I express my sincere thanks to my son Shouryaa who has changed my perspective towards life and given it a direction. He is my biggest supporter and critique and because of him I am able to live up to my aspirations. He has been my best buddy in this journey so far. I am indebted to my Parents (K.N. Sharma and Saroj Sharma) for showering unconditional love. My special thanks to my husband Rohit for always encouraging me to attain my professional goals, he is the very essence of my life. My gratitude and love to my brother Sadashiv and my sister-in-law Shipra who have always provided me support in thick and thin. I am also grateful to soul mates Dr. Kriti Priya, Shilpee Sharma and Neetu Gupta for being my life anchor and stabilizer. I am thankful to my students Dr. Arjun Sirohi, Dr. Anuradha Pughat, Dr. Gayatri Sakya, Dr. Gourav Verma, Dr. Neeti Bansal, Dr. Aarti Gautam Dinkar, Gamini Joshi, Monika Kashyap, and Zaineb Naaz for always standing by my side. I am indebted to Dr. Neeta Singh, Dr. Navaid Zafar Rizvi, Dr. Vimlesh, Dr. Rajesh Mishra, Dr. Madhu Jain, and Prof. G.C. Sharma for helping me in my academic journey.

I am thankful to BPB Publications for their support and help in framing this book and I hope our readers will use it to further enhance their knowledge and attain their career goals.

Thanks & Regards
Dr. Vidushi Sharma

- ❖ I would like to extend my sincere thanks to some people who have generously contributed and supported me in writing and presenting this book. First and foremost, I would like to thank my parents and parents-in-law for continuously encouraging and supporting me. Next, I owe my gratitude to my supervisor Dr. Vidushi Sharma, for her valuable guidance, constructive comments and continuous encouragement throughout my book. I feel overwhelmed to spell some of my guiding force - my brother Gaurav Joshi and his wife Vandana Upadhyaya, my sister-in-law Dr. Meenakshi Lohani, and my friends Sunita Mishra and Sharad Rai. Last but not least, my loving and supporting husband Mr. Mani Lohani and my darling daughter Mishthi. I could have never completed this book without their support.

My gratitude also goes to the team at BPB Publications for being supportive enough to provide me enough time to finish and publish the book. At last, I would like to thank God who gave me enough strength and patience to write such a detailed book on IoT security. Hope this book brings wonderful joy and experience to readers worldwide.

Thanks & Regards

Gamini Joshi

Preface

Internet of Things is an emerging technology, which has changed our life from smart homes to smart defense to smart industrial applications. Criticality of these applications has led to an intense need to provide security, safety and privacy to these applications and shield them from awful threats and attacks. In connection with this, the book “**Enhancing IoT Security**” is presented, that aims to introduce the next generation security measure for Internet of Things (IoT) with their permissive security technologies and applications to a wide interdisciplinary readership of engineering and non-engineering graduate students, post-graduate students and researchers.

This book aims to reveal the importance of IoT security and introduces the efficient technique that effortlessly recognizes the existing threats and attacks with their impressive solutions of mitigating them. Its ambition is to secure resource constraint sensor enabled IoT networks and devices at minimal cost concerning complexity, energy and power. This book intends to analyze the critical application areas where security and privacy are indispensable. It includes theoretical as well as practical aspect of securing network with empirical IoT products (hardware) and simulators (software). In doing so, this book destines the target readers to move beyond their theoretical knowledge and include features of practicality that triggers new experiments and multidisciplinary project ideas. Moreover, authors in this book have illustrated their teaching and research experience which would assist the academician and researchers in extending their research and studies in right direction.

This book fulfills the basic and advanced level need of the readers related to the topic it covers. The book is self-satisfied for the topics it covers and contains the detailed as well as advances knowledge on security issues in IoT networks.

Apart from the detailed text, the book includes figures, tables, graphs (real-time and lab results), case studies and examples too. For assessing the knowledge of the readers, Questionnaire including multiple choice questions, short and long answer questions is given at the end of each chapter. Each chapter starts with an introduction of the topic and discusses its related issues and future directions to the work in that specified area. The details of every chapter are listed below:

Chapter 1- The Internet of Things and its Security Requirements: It gives the basic architecture of IoT and fulfills the requirement of preliminary knowledge for subsequent chapters. Though IoT is changing everything; yet industries, consumers, and technology owners are under security nightmare since smart devices and infrastructures are giving frenzy opportunity to cyber-criminals. This states that IoT security is clearly an important aspect; diving into it this chapter explores the need of security in IoT and its requirement with respect to architecture, devices, and protocols. This continues with the range of security applications within the specific domain like SCADA system, enterprise system, agriculture system and much more. In the next section of this chapter, the need of securing IoT databases is discussed with advanced technologies like embedded systems, bigdata analytics, cloud, fog and edge computing

Chapter 2- IoT Security - Vulnerabilities, Attacks, and Countermeasures: It explores different types of vulnerabilities, attacks and risk against IoT implementations and deployments. This chapter dives into the organization of attack and illustrates how attacks are organized into attack and fault tree. Next, the access control techniques with their different types are investigated and systematic methodology for incorporating countermeasures against attacks is talked about. Thereafter, the chapter provides the tailored approach to threat modeling that demonstrates the method of identifying threats and its sources with their procedure of mitigating them. We have explained it with the help of suitable examples.

Chapter 3- Security Engineering for IoT Development: After discussing the IoT security requirements and the threats affecting the security of the system. We now investigate the security engineering for IoT development, where various tools and methodology are discussed that is implemented on IoT system during its designing and development phase. This chapter presents the different phases of designing security into exiting system which involves planning, selection, processing, and development methodology.

Chapter 4- IoT Security Lifecycle: In continuation with chapter 3, in this chapter we will present the complete lifecycle of IoT security, which involves secure designing, implementation, integration, operation, maintenance and dispose. Each phase is discussed in detail with every perspective of securing IoT.

Chapter 5- IoT as Interconnection of Threats: Next, we present the interconnection of threats in IoT applications and the methods to secure them. This chapter presents

various fusion schemes, defense scheme and solution-based analyses of detecting attack vectors like Sybil attack and malwares in smart vehicular and home systems.

Chapter 6- Crypto Foundations I: It explores the role of cryptography in engineering IoT security. It includes the cryptographic primitives, modules, principles and fundamentals, which encompasses MAC codes, Hash codes, signature codes and various cipher suites. We have also included various key management algorithms with their fundamental and advanced schemes. Next, the chapter examines transport encryption and cryptographic controls for IoT communication and messaging protocols. Last but not the least, we have also discussed light weighted cryptographic technique for authenticating IoT Node.

Chapter 7- Crypto Foundations II: This chapter is in continuation to chapter 6. It extends the concept of cryptography with hash function and digital signature. It also provides an in-depth illustration of how cryptography can be used to protect IoT communications and its messaging protocols. The chapter outlines the cryptographic controls for IoT communication and messaging protocols, along with the IoT node authentication mechanisms.

Chapter 8- Privacy Preservation for the Internet of Things: In this chapter, we present the privacy preserving schemes for IoT systems. It explores the Privacy preservation Data Dissemination problem with its spatial privacy graph (SPG) solution. Privacy preservation is further explored with the help of real time example of smart buildings where the concept of IoT in smart building is explained with possible threats and its solution approaches.

Chapter 9- Location Privacy Enhancement in the Internet of Vehicles: This chapter further explores the privacy preservation with yet another smart example in Internet of vehicles. Since Vehicles are mobile the focus of this chapter is on location privacy. This chapter explores location privacy requirements with preservation schemes and protocols. Further, the security analysis is presented with performance evaluation.

Chapter 10- Privacy Protection in Key Personal IoT Applications: Since IoT devices and systems are resource constraint, there is always a need to have light weighted algorithms. In connection with it, this chapter presents a lightweight and robust scheme for privacy protection in mobile WBSN and Participatory Sensing network.

Chapter 11- Trust and Trust Models for the IoT: It presents another aspect of securing IoT system, that is, using Trust as the parameter of protecting IoT network and devices. This chapter explores the concept of trust model and its perspective of securing IoT. It also explores Trust models with the help of example scenarios.

Chapter 12- Framework for Privacy and Trust in IoT: This chapter explores trust and its framework in decentralized IoT system. Framework presents user centric as well as device centric framework with Face-to-face enabler as well as Indoor localization enabler tool.

Chapter 13- Preventing Unauthorized Access to Sensor Data and Authentication in IoT: Authentication is yet another issue in IoT system. In regard with this, the chapter illustrates the fundamentals of authentication with detailed study of message and entity authentication. It also explores the cooperative authentication scheme using Game modeling where players, strategies and utility function are illustrated with respect to cooperative authorization with experimental results and analysis.

Chapter 14- Computational Security for the IoT and Beyond: IoT systems are very complex systems. Considering this, the chapter explores the characteristics of complex IoT systems like wireless networks, biological networks, social networks, economic networks and heavy computer networks. Further, the complexity of these networks is evaluated with the help of computational tools like, signal processing, and network science tools. The controllability and observability of networks is further studied from communication engineering.

Chapter 15- Identity and Access Management Solutions for the IoT: This chapter explores the issue of identification and access management of IoT devices and network in different environment and organization. This chapter reviews the identity lifecycle and discusses the infrastructure components needed for provisioning authentication credentials. It focuses on authentication credentials and its approaches of providing authorization and access controls to IoT devices.

Chapter 16- Privacy-Preserving Time Series Data Aggregation for IoT: This chapter describes the concept of data aggregation in IoT network for preserving network privacy. System and security models are detailed out and a time-series data aggregation schemes is presented for preserving IoT network and security analysis with performance evaluation is showed in terms of computational and communication cost.

Chapter 17- Path Generation Scheme for Real-Time Green IoT: This chapter investigates the issue of secure routing in IoT network. It presents the secure path generation scheme for real-time Green Internet of Things. Network model and problem definitions are deeply discussed and then a framework of path generation is established with all security measures.

Chapter 18- Security Protocols for IoT Access Networks and Their Impact on Mobile Networks: This chapter presents the detailed study of existing security protocols and its impact on mobile networks. It also investigates the scalability issue in large cellular network. The chapter presents the unidirectional and bidirectional data transmission security algorithm.

Chapter 19- Cloud Security for the IoT: This chapter presents the prospect of cloud security designed for Internet of Things. It addresses cloud services and IoT related internal and external threats. It explores the cloud service providers for IoT and their security-as-a-service. The chapter also examines the security functionality needed from cloud for building an effective IoT architecture. Lastly, it discusses and explores new computing paradigms that cloud could provide to IoT system.

Chapter 20- Policy-Based Approaches for Informed Consent in IoT: This chapter gives a detailed description about policy based approaches for Internet of Things. It provides the framework and enforcement policy with their future developments.

Chapter 21- Blockchains for Internet of Things: This chapter presents the blockchain technique as next generation technology for securing Internet of Things. It addresses the concept of bitcoin, crypto-currency and other matter of concern for Internet of Things.

Chapter 22- Game Theory Foundation: This chapter introduces the concepts and techniques of Game Theory. The mathematical formulations of the game along with its strategy are detailed out. We present different types of games and its strategic approach like repeated games, Bayesian games and coalitional games that will help readers to justify their problems.

Chapter 23- Security Products: In this chapter, we have presented the recent trends of securing Internet of Things where existing security products and their test beds are discussed. We have also illustrated the commercialized IoT products and their usage.

Coloured Images

Please follow the link to download the
Coloured Images of the book:

<https://rebrand.ly/lсыz3qa>

We have code bundles from our rich catalogue of books and videos available at <https://github.com/bpbpublications>. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Did you know that BPB offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.bpbonline.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at :

business@bpbonline.com for more details.

At **www.bpbonline.com**, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on BPB books and eBooks.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at business@bpbonline.com with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit www.bpbonline.com. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit www.bpbonline.com.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

<https://discord.bpbonline.com>



Table of Contents

1. The Internet of Things and its Security Requirements.....	1
Structure.....	2
1.1 Internet of Things - A brief introduction.....	2
1.1.1 <i>Growth trends and market opportunity</i>	3
1.2 Networking in the IoT device - The framework.....	5
1.2.1 <i>Identification</i>	5
1.2.2 <i>Sensing</i>	7
1.2.3 <i>Communication</i>	8
1.2.4 <i>Computation</i>	9
1.2.5 <i>Services</i>	9
1.2.6 <i>Semantics</i>	10
1.3 Need to secure IoT - Its limitations.....	11
Reason 1 - <i>Constrained system resources</i>	12
Reason 2 - <i>Device Heterogeneity</i>	13
Reason 3 - <i>Interoperability in IoT</i>	13
Reason 4 - <i>Over-the-Air firmware update</i>	13
1.4 Cyber security versus IoT security and cyber-physical systems.....	14
1.5 IoT architecture.....	15
Layer 1 - <i>Perception/Sensing layer</i>	16
Layer 2 - <i>Network layer</i>	16
Layer 3 - <i>Service/Processing layer</i>	16
Layer 4 - <i>Application/Interface layer</i>	17
1.5.1 <i>Security threats in IoT architecture layers</i>	17
1.5.2 <i>Security requirements in IoT architecture layers</i>	21
1.6 Authorization and authentication requirement in IoT.....	23
1.6.1 <i>Insufficient authentication/authorization in IoT</i>	25
1.7 Security in enabling technologies behind the Internet of Things.....	26
1.7.1 <i>Security in hardware technologies - Identification</i>	26
1.7.2 <i>Security in software technologies: Integration of WSN and RFID</i>	27
1.7.3 <i>Security in communication technologies - tracking, monitoring, and communicating</i>	28
<i>Security in network technologies: network function</i>	29

1.8 IoT networking protocols and its security	30
1.8.1 Application protocol.....	30
1.8.2 Network Layer Protocols: 6LoWPAN	33
1.8.3 Routing /Transport Layer Protocol - RPL	34
1.8.4 Link Layer Protocol: IEEE 802.15.4	35
1.8.5 Physical Layer Protocol - LTE-A, Z-Wave	35
1.9 Domain-specific IoT and its security concerns.....	36
1.9.1 Security concerns in SCADA systems	36
1.9.2 Security concerns in Enterprise Information Systems	38
1.9.3 Security concerns in home automation.....	39
1.9.4 Security concerns in agriculture.....	39
1.9.5 Security concerns in smart cities.....	40
1.9.6 Security concerns in social IoT.....	41
1.9.7 Security concerns in IoT-based healthcare	42
1.10 IoT supporting technologies	42
1.10.1 Big Data analytics.....	43
1.10.2 Cloud computing.....	43
1.10.3 Edge computing	45
1.10.4 Fog computing	46
Conclusion.....	47
1.11 Questionnaire	49
Multiple choice questions.....	49
Answer key	51
Long answer questions.....	51
Short answer questions	51
Keywords(F.....	52
References.....	53
Things to check before moving to next chapter	55
2. IoT Security - Vulnerabilities, Attacks, and Countermeasures.....	57
Introduction.....	57
Structure.....	57
2.1 Information Assurance: components.....	58
2.2 Threats.....	60
Associated terms	60

<i>Threat classification</i>	60
2.3 Vulnerabilities	62
2.4 Risk	63
2.5 Insecure Access control	63
2.5.1 <i>Access Control List-Based Systems or Discretionary Access control</i>	64
2.5.2 <i>Role-Based Access control</i>	64
2.5.3 <i>Capability-Based Access control or Key-based Access control system</i>	64
2.5.4 <i>Challenges in Access control</i>	64
2.5.5 <i>Threats to Access control, privacy, and availability</i>	65
2.6 Attacks: types, composition, and tools	66
2.6.1 <i>Types of attacks</i>	67
2.6.2 <i>Tools for attack identification</i>	70
2.7 Threat modeling for IoT systems	78
Conclusion	86
2.8 Questionnaire	90
<i>Multiple choice questions</i>	90
<i>Answer key</i>	90
<i>Long answer question</i>	91
<i>Short answer questions</i>	91
Keywords E F	91
References	92
Things to check before moving to the next chapter	92
3. Security Engineering for IoT Development	93
Introduction	93
Structure	94
3.1 Building Security into design and development	94
3.1.1 <i>Managing security requirement</i>	94
3.1.2 <i>Managing security in IoT when in operation</i>	95
3.2 The IoT security life cycle: Secure design	97
<i>Phase 1: Secure design</i>	98
3.2.1 <i>Safety and security design</i>	99
3.2.2 <i>Processes and Agreements</i>	110
3.2.3 <i>Technology selection: Security products and services</i>	115
Conclusion	123

3.3 Questionnaire.....	124
<i>Multiple choice questions</i>	124
<i>Answer key</i>	125
<i>Long answer question</i>	125
<i>Short answer questions</i>	126
Keywords E F.....	126
References.....	127
Things to check before moving to the next chapter.....	128
4. IoT Security Lifecycle	129
Structure.....	129
4.1 Introduction.....	130
4.2 Phase 2: Implementation and Integration.....	130
4.2.1 <i>IoT Security CONOPS document</i>	131
4.2.2 <i>Network implementation and security integration</i>	132
4.2.3 <i>System security verification and validation (V&V)</i>	135
4.2.4 <i>Security training</i>	135
4.2.5 <i>Secure configurations</i>	136
4.3 Phase 3: Operations and maintenance.....	137
4.3.1 <i>Managing identities, roles, and credentials</i>	138
4.3.2 <i>Security monitoring</i>	140
4.3.3 <i>Penetration testing</i>	141
4.3.4 <i>Asset and configuration management</i>	143
4.3.5 <i>Incident management</i>	143
4.3.6 <i>Forensics</i>	144
4.4 Phase 4: Dispose.....	144
4.4.1 <i>Secure device disposal and zeroization</i>	145
4.4.2 <i>Data purging</i>	145
4.4.3 <i>Inventory control</i>	145
4.4.4 <i>Data archiving and records management</i>	146
<i>Conclusion</i>	146
4.5 Questionnaire.....	147
<i>Multiple choice questions</i>	147
<i>Answer key</i>	148
<i>Long answer question</i>	148

<i>Short answer questions</i>	149
Keywords E F.....	149
References.....	149
Things to check before moving to the next chapter.....	150
5. IoT as Interconnection of Threats	151
Structure.....	152
5.1 Sybil Attack Detection in Vehicular Network.....	152
5.1.1 <i>Concept of a Vehicular Network or a Vehicular Ad-Hoc Network</i>	152
5.1.2 <i>Challenges and Attacks in Vehicular Network</i>	154
5.1.3 <i>Consequences of a Sybil attack</i>	156
5.1.4 <i>Sybil Attack Detection Schemes in a VANET Network</i>	157
5.2 Malware Propagation and control in Internet of Things	164
5.2.1 <i>Malware in Internet of Things</i>	164
5.2.1 <i>Modeling of malware propagation</i>	165
5.2.3 <i>Malware control strategy</i>	170
5.3 Solution-based analysis of attack vectors on smart home systems.....	171
5.3.1 <i>Concept of a Smart Home System with an example of digitalSTROM</i>	172
<i>Technical Structure of digitalSTROM(dS)</i>	173
5.3.2 <i>Attack vectors on SHS</i>	174
<i>Central digitalSTROM Server</i>	174
<i>Smart control devices</i>	175
<i>Smart home communication bus</i>	175
<i>Remote third-party services</i>	176
5.3.3 <i>SHS Hardening</i>	176
<i>Hardening of Central digitalSTROM server</i>	176
<i>Hardening of Smart Control Devices</i>	177
<i>Hardening of Smart Communication Bus</i>	177
<i>Hardening of remote third-party services</i>	178
5.3.4 <i>Attack scenario and its solution analysis</i>	178
<i>Attack 1</i>	178
<i>Attack 2</i>	179
5.4. Network robustness of the Internet of Things.....	179
5.4.1 <i>Network Robustness using Game-Theoretic analysis</i>	180
Conclusion.....	183

5.5 Questionnaire.....	185
<i>Multiple choice questions</i>	185
<i>Answer key</i>	186
<i>Long answer questions</i>	186
<i>Short answer questions</i>	186
Keywords E F.....	186
References.....	187
Things to check before moving to the next chapter.....	189
6. Crypto Foundations I.....	191
Structure.....	191
6.1 Cryptography and its role in securing the IoT.....	192
6.2 Cryptography and its primitives in the IoT.....	193
<i>Cryptographic primitives</i>	194
6.3 Secrecy and secret-key capacity in IoT.....	195
<i>Secret key capacity</i>	195
6.4 Encryption and decryption.....	197
6.4.1 <i>Symmetric key encryption algorithm</i>	198
<i>Substitution technique</i>	199
<i>Transposition technique</i>	213
<i>Electronic Code Book</i>	228
<i>Cipher Block Chaining Mode</i>	228
<i>Cipher Feedback Mode</i>	229
<i>Output Feedback Mode</i>	231
<i>Counter Mode</i>	232
6.4.2 <i>Asymmetric key encryption algorithm</i>	233
Conclusion.....	236
6.5 Questionnaire.....	237
<i>Multiple choice questions</i>	237
<i>Answer key</i>	238
<i>Long answer questions</i>	238
<i>Short answer questions</i>	238
Keywords E F.....	238
References.....	239

7. Crypto Foundations II.....	241
Structure.....	241
7.1 Message integrity- Hash functions and their security	242
7.1.1 <i>Properties and applications of Hash functions.....</i>	242
<i>Applications of the Hash function</i>	243
7.1.2 <i>Popular Hash function.....</i>	245
7.1.3 <i>Merkle tree.....</i>	249
<i>Significance of the Merkle tree.....</i>	250
7.2 Message authentication	252
7.2.1 <i>Message Authentication Code.....</i>	253
7.2.2 <i>Authenticated encryption</i>	254
7.3 Random number generation	257
7.4 Cipher suites.....	259
7.5 Signature algorithm means of IoT node authentication	260
7.5.1 <i>Types of signatures.....</i>	261
7.5.1 <i>Digital signature schemes.....</i>	262
7.6 Cryptographic key management.....	268
7.6.1 <i>Key management fundamentals.....</i>	268
7.6.2 <i>Diffe-Hellman key exchange</i>	273
<i>Algorithm.....</i>	273
7.6.3 <i>Elliptic Curve Cryptography</i>	275
<i>Background explanation of ECC.....</i>	276
<i>ECC algorithm for key-exchange.....</i>	276
<i>ECC Algorithm for encryption and decryption.....</i>	277
7.6.4 <i>Public Key Infrastructure</i>	278
<i>PKIX Model.....</i>	279
<i>PKIX Management function</i>	280
7.7. Examining cryptographic controls for IoT protocols	280
7.7.1. <i>Cryptographic controls built into IoT communication protocols</i>	281
<i>ZigBee.....</i>	281
<i>Bluetooth-LE.....</i>	282
<i>Near Field Communication</i>	283
7.7.2 <i>Cryptographic controls built into IoT messaging protocols.....</i>	283
7.8 Transport encryption.....	284
7.8.1 <i>Transport Layer Security.....</i>	284

7.8.2 <i>Secure Sockets Layer</i>	286
7.8.3 <i>HTTPS</i>	287
Conclusion	287
7.9 Questionnaire	288
<i>Multiple choice questions</i>	288
<i>Answer key</i>	289
<i>Long answer questions</i>	289
<i>Short answer questions</i>	289
Keywords E F	289
References	289
Things to check before moving to the next chapter	290
8. Privacy Preservation for the Internet of Things	291
Structure	291
8.1. Privacy preservation	292
8.2. Classification of privacy threats in IoT	293
8.2.1. <i>Content-oriented privacy threats</i>	293
8.2.2. <i>Contextual-oriented privacy threats</i>	294
8.3. Privacy preservation techniques	294
8.3.1. <i>Cryptographic techniques</i>	296
8.3.2. <i>Anonymization techniques</i>	296
<i>K-anonymity</i>	296
<i>L diversity</i>	298
8.3.3. <i>Dynamic data masking</i>	298
8.4. Futuristic approach of privacy preservation data dissemination	299
8.4.1. <i>Pre-requirements of the approach</i>	300
<i>Network model</i>	300
<i>Threat model</i>	301
<i>Resolution of uncertainty</i>	302
<i>The objective of the FDD approach</i>	305
8.4.2. <i>Implementation of the privacy preservation data dissemination approach</i>	307
<i>SPG-based data dissemination</i>	307
8.5. Privacy preservation for IoT used in smart buildings- A case study	313
8.5.1. <i>The concept of smart buildings</i>	313
<i>Smart Building Subsystems</i>	314

IoT Technologies used in smart buildings	316
8.5.2. Privacy threats in smart buildings	316
8.5.3 Privacy-preserving approaches in smart buildings	318
Wireless LAN privacy-preserving approaches.....	318
RFID privacy-preserving approaches	320
Video surveillance privacy-preserving approaches.....	321
Conclusion.....	323
8.6 Questionnaire.....	324
Multiple choice questions.....	324
Answer key	325
Long answer questions.....	325
Short answer questions.....	325
Keywords E F.....	325
References.....	326
Things to check before moving to the next chapter.....	326
9. Location Privacy Enhancement in the Internet of Vehicles.....	327
Structure.....	327
9.1. Location privacy and its requirements in IoV	328
9.1.1. Location-privacy requirements	328
9.2. Traditional location-privacy preservation solutions.....	329
9.2.1. Pseudonyms	329
9.2.2. Mix-Zone	330
9.2.3. Group signature.....	331
9.2.4. Silent period	331
9.3. A new location-privacy preservation scheme: A MixGroup approach....	332
9.3.1. Pre-requirements of the MixGroup approach	333
Network model	333
Social model	335
Threat model.....	336
Characteristics of the vehicular social network	337
Some observations from the traces of vehicles.....	337
Theory of MixGroup	338
9.3.2. Process of MixGroup.....	341
System initialization and key generation	341

Group join.....	342
Pseudonym exchange.....	343
RSU signing protocol.....	343
Group leaving.....	344
Revocation protocol.....	344
9.3.3. Security analysis.....	345
Conditional tracking.....	345
Attack and defense analysis.....	346
Entropy optimal pseudonym exchange.....	347
9.3.4. Experimental analysis of the MixGroup approach.....	349
Conclusion.....	352
9.4. Questionnaire.....	353
Multiple choice questions.....	353
Answer key.....	354
Long answer questions.....	354
Short answer questions.....	354
Keywords E F.....	354
References.....	354
Things to check before moving to the next chapter.....	355
10. Privacy Protection in Key Personal IoT Applications.....	357
Structure.....	358
10.1. Concept of personal IoT.....	358
10.1.1. Mobile WBSN.....	359
Architecture of WBSN.....	359
Issues in mobile WBSN.....	360
10.1.2. Participatory sensing.....	361
Architecture of Participatory Sensing.....	361
Issues in participatory sensing.....	362
10.2. Security aspect of personal IoT.....	363
10.2.1. Lightweight and robust schemes for protecting privacy in Mobile WBSN.....	363
10.2.1.1. One Time Mask scheme.....	365
10.2.1.2. One Time Permutation scheme.....	366
10.2.1.3. Comparative analysis of OTM and OTP.....	368

10.2.2. <i>Lightweight and robust scheme for privacy protection in participatory sensing</i>	368
10.2.2.1. <i>The LRTP scheme</i>	369
Conclusion.....	375
10.3 Questionnaire	376
<i>Multiple choice questions</i>	376
<i>Answer key</i>	377
<i>Long answer questions</i>	377
<i>Short answer questions</i>	377
Keywords E F.....	377
References.....	377
Things to check before moving to the next chapter.....	378
11. Trust and Trust Models for the IoT	379
Structure.....	379
11.1. Concept of trust and its role in securing IoT.....	380
11.2. A brief study on Trust Management System.....	381
11.2.1. <i>Information gathering</i>	381
11.2.2. <i>Trust computation</i>	381
11.2.3. <i>Trust propagation</i>	382
11.2.4. <i>Trust update</i>	382
11.3. Classification of Trust Management Systems in IoT network.....	383
11.3.1. <i>Layered architecture</i>	383
<i>a. Device layer</i>	383
<i>b. Support layer</i>	384
<i>c. Other layers</i>	385
11.3.2. <i>Propagational architecture</i>	385
<i>a. Distributed architecture</i>	385
<i>b. Centralized architecture</i>	386
11.3.3. <i>Conceptual architecture</i>	388
<i>a. Direct trust model</i>	388
<i>b. Indirect trust model</i>	389
11.4. Challenges in existing trustable IoT techniques.....	389
11.4.1. <i>Naming and name resolution</i>	389
11.4.2. <i>Identifier/locator splitting</i>	391

11.4.3. <i>Availability of resources and services</i>	391
11.4.4. <i>Security and privacy</i>	392
11.5. <i>Introducing Nova-Genesis as an IoT architecture</i>	393
11.5.1. <i>Naming and name resolution</i>	393
11.5.2. <i>Identifier/locator splitting</i>	394
11.5.3. <i>Availability of resources and services</i>	395
11.5.4. <i>Security and privacy</i>	398
Conclusion.....	399
11.6. <i>Questionnaire</i>	400
<i>Multiple choice questions</i>	400
<i>Answer key</i>	401
<i>Long answer questions</i>	401
<i>Short answer questions</i>	401
Keywords E F.....	401
References	401
Things to check before moving to the next chapter.....	402
12. Framework for Privacy and Trust in IoT	403
Structure.....	403
12.1. <i>The concept of user-centric Internet of Things</i>	404
12.1.1. <i>Internet of People</i>	404
12.1.2. <i>Social Internet of Things</i>	405
<i>Basic components of SIoT</i>	405
12.1.3. <i>Physical Cyber Social Computing</i>	406
12.1.4. <i>People as a Service</i>	406
12.1.5. <i>Advantages of user-centric Internet of Things</i>	407
12.2. <i>Issues in user-centric Internet of Things</i>	407
12.2.1. <i>Utility and usability</i>	407
12.2.2. <i>Fault tolerance</i>	408
12.2.3. <i>Interoperability, data-models, and nomenclatures</i>	408
12.2.4. <i>Big data (graph) analysis</i>	408
12.2.5. <i>Trust and privacy</i>	408
12.3. <i>SocIoTal- A socially aware citizen-centric Internet of Things</i>	409
12.3.1. <i>Classical IoT-architectural framework</i>	410
<i>Core component</i>	411

12.3.2. SocIoTal security framework.....	413
12.3.2.1. Authentication.....	414
12.3.2.2. Trust and reputation.....	415
12.3.2.3. Key-exchange management	415
12.3.2.4. Context manager.....	416
12.3.2.5. Identity management.....	418
12.3.2.6. Authorization.....	421
12.3.2.7. Group manager	423
Conclusion.....	425
12.4. Questionnaire.....	426
Multiple choice questions.....	426
Answer key	427
Long answer questions.....	427
Short answer questions.....	427
Keywords E F.....	427
References.....	428
Things to check before moving to the next chapter.....	428
13. Preventing Unauthorized Access to Sensor Data and Authentication in IoT ...	429
Structure.....	430
13.1 The idea of cooperation in IoT.....	430
13.1.1. Cooperative communication.....	430
13.1.2. Cooperative authentication	431
13.1.3. Cooperative incentive.....	432
13.1.4. Conflict balancing	433
13.2. The practical implementation of cooperative authentication	433
13.3. Bargaining-based dynamic game model for cooperative authentication ...	435
13.3.1. The pre-requisite of the cooperative authenticated bargaining system	436
13.3.1.1. Factors affecting the price.....	436
13.3.1.2. Bargaining-based price	438
13.3.1.3. Bargaining procedure.....	439
13.3.2. The dynamic game.....	440
Players	440
Strategy	440
Utility function.....	441

<i>Performance of the bargaining-based dynamic game model for cooperative authentication</i>	442
13.3.3.1. <i>Location privacy leakage</i>	442
13.3.3.2. <i>Energy consumption</i>	443
13.3.3.3. <i>Network survivability</i>	444
13.4. <i>Analysis of dynamic game model for cooperative authentication</i>	445
13.4.1. <i>Dynamic game with complete information</i>	446
13.4.2. <i>Dynamic game with incomplete information</i>	448
13.5. <i>Variants of entity authentication</i>	453
a. <i>Reputation</i>	453
b. <i>Vote</i>	454
c. <i>Abstinence</i>	454
d. <i>Police</i>	454
13.5.1. <i>Performance analysis of the variants of entity authentication</i>	454
a. <i>Average vulnerability time</i>	455
b. <i>Average risks</i>	456
13.6. <i>Message authentication: content delivery in VANET</i>	457
13.6.1. <i>Voting on reputation for VANET(VOR4VANET)</i>	458
Conclusion.....	459
13.7. <i>Questionnaire</i>	462
<i>Multiple choice questions</i>	462
<i>Answer key</i>	463
<i>Long answer questions</i>	463
<i>Short answer questions</i>	463
Keywords E F.....	463
References.....	463
Things to check before moving to the next chapter.....	463
14. Computational Security for the IoT and Beyond	465
Structure.....	465
14.1. <i>An introduction to computational models and their security</i>	466
14.1.1. <i>Need for computational security in the Internet of Things</i>	466
14.2. <i>Complex systems</i>	467
14.2.1. <i>Characteristics of complex systems</i>	468
<i>IoT as a complex system</i>	468

14.2.2. Security challenges in complex systems	470
14.3. Examples of complex systems with their security characteristics.....	471
14.3.1. Wireless networks.....	471
14.3.2. Social networks.....	471
a. Multimedia content threats	472
b. Traditional threats.....	472
c. Social threats	472
14.3.3. Economic networks	473
14.3.4. Computer networks.....	473
14.4. Computational tools for complex systems.....	474
14.4.1. Signal processing tools.....	474
14.4.2. Network science tools	475
14.4.3. Controllability and observability of networks.....	476
14.4.4. Network tomography	476
14.5. Future scope	477
Conclusion.....	478
14.6 Questionnaire.....	479
Multiple choice questions.....	479
Answer key	480
Long answer questions.....	480
Short answer questions.....	480
Keywords E F.....	480
References	480
Things to check before moving to the next chapter.....	481
15. Identity and Access Management Solutions for the IoT.....	483
Structure.....	483
15.1. Introduction to identity and access management for the IoT	484
Implementation of IAM for the development of IoT application.....	485
a. Default password risks.....	486
b. Cross-domain IoT.....	486
c. Credential abuse.....	486
d. Virtual Eavesdropping.....	486
15.2. The identity lifecycle	487

15.2.1. Identity establishment with unique requirements	488
Identity of IoT devices.....	488
15.2.2. Secure bootstrap.....	488
Bootstrapping using PKI.....	489
15.2.3. Credential and attribute provisioning.....	490
15.2.4. Account monitoring and control.....	491
15.2.5. Account updates.....	492
15.2.6. Account suspension	492
15.2.7. Account/credential deactivation/deletion.....	492
15.3. Authentication credentials	492
15.3.1. Usernames and passwords.....	493
15.3.2. Symmetric keys	493
15.3.3. Certificates.....	493
X.509.....	494
IEEE 1609.2.....	494
15.3.4. Biometrics	494
15.3.5. New work in authorization for the IoT	495
15.4. IoT IAM infrastructure.....	495
15.4.1. PKI for the IoT IAM	495
Revocation support.....	496
15.5. Authorization and access control.....	497
15.5.1. OAuth 2.0.....	497
OAuth2.0 components.....	497
Working of OAuth2.0	498
15.5.2. Access controls within publish/subscribe protocols.....	499
15.5.3. Access controls within communication protocols.....	499
Conclusion.....	499
15.6. Questionnaire	500
Multiple choice questions.....	500
Answer key.....	501
Long answer questions.....	501
Short answer questions.....	501
Keywords E F.....	502
References	502
Things to check before moving to the next chapter.....	502

16. Privacy-Preserving Time Series Data Aggregation for IoT	503
Structure.....	503
16.1 Data aggregation on IoT system.....	504
16.1.1 <i>Data aggregation mechanisms on IoT system</i>	504
16.1.1.1 <i>Client-server-based data aggregation mechanisms</i>	505
16.1.1.2 <i>Mobile-agent-based data aggregation mechanisms</i>	506
16.1.1.3 <i>Time-series-based data aggregation mechanisms</i>	506
16.2 Time-series data aggregation privacy preservation scheme	507
16.2.1 <i>Prerequisites</i>	507
IoT scenario.....	507
Security consideration and design goals.....	508
Properties of the Group Z_p^*	509
16.2.2 <i>The actual scheme</i>	510
System settings.....	510
Data encryption at nodes.....	510
Data aggregation at gateways	510
Aggregated data decryption at the control center.....	511
Privacy maintenance during node joining and leaving	512
16.2.3 <i>Computational cost of time series data aggregation privacy preservation scheme</i>	513
Conclusion.....	514
16.3 Questionnaire	515
Multiple choice questions.....	515
Answer key	515
Long answer question	516
Short answer question.....	516
Keywords E F.....	516
References	516
Things to check before moving to the next chapter.....	516
 17. Path Generation Scheme for Real-Time Green IoT	 517
Structure.....	518
17.1 Green Internet of Things: An introduction	518
17.1.1 <i>GIoT components</i>	519
a. <i>Green hardware</i>	519

<i>b. Green software</i>	520
<i>c. Green communication</i>	520
<i>d. Green architecture</i>	520
17.1.2 <i>Green IoT technologies</i>	521
<i>Green tags</i>	521
<i>Green sensing networks</i>	522
<i>Green cloud computing</i>	522
<i>Green coding</i>	522
<i>Green data centers</i>	523
<i>Green M2M</i>	523
17.1.3 <i>Contribution toward Green IoT</i>	524
17.1.4 <i>GIoT open issues</i>	524
<i>a. Technical challenges</i>	525
<i>b. Standardization</i>	525
<i>c. Security and privacy</i>	525
17.2 <i>Real-time GIOT and its issues</i>	526
17.3 <i>Real-time query processing in the Green Internet of Things</i>	527
17.3.1 <i>Query processing in the green Internet of Things</i>	528
<i>Mathematical representation of query processing</i>	529
17.3.2 <i>Secure path generation scheme</i>	531
<i>Procedure for the generation of GIoT secured path</i>	532
<i>Example: Derivation of Query Execution Path</i>	535
Conclusion.....	539
17.4 <i>Questionnaire</i>	540
<i>Multiple choice questions</i>	540
<i>Answer key</i>	540
<i>Long answer question</i>	540
<i>Short answer questions</i>	541
Keywords E F.....	541
References.....	541
Things to check before moving to the next chapter.....	541
18. Security Protocols for IoT Access Networks and Their Impact on Mobile Networks	543
Structure.....	544

18.1. Existing security features of IoT protocols.....	544
18.2. Futuristic security protocol / algorithm for IoT network	546
18.2.1. <i>Time-based secure key generation and renewal</i>	546
a. <i>Security protocol for unidirectional data transmissions</i>	548
b. <i>Security protocol for bidirectional data transmissions</i>	550
18.2.2 <i>Cognitive security</i>	550
18.3 Impact of IoT security on mobile networks	552
<i>Cost of mobile network</i>	552
<i>The risk and complexity of mobile networks</i>	553
<i>Delay in mobile network</i>	553
<i>Scope restriction of mobile network</i>	553
Conclusion.....	553
18.4 Questionnaire.....	554
<i>Multiple choice questions</i>	554
<i>Answer key</i>	555
<i>Long answer question</i>	555
<i>Short answer questions</i>	555
Keywords E F.....	556
References.....	556
Things to check before moving to the next chapter.....	556
19. Cloud Security for the IoT	557
Structure.....	558
19.1. Cloud services and the IoT.....	558
19.1.1. <i>Samples of IoT cloud services</i>	558
a. <i>Asset/inventory management</i>	558
b. <i>Service provisioning, billing, and entitlement management</i>	559
c. <i>Real-time monitoring</i>	559
d. <i>Sensor coordination</i>	559
e. <i>Customer intelligence and marketing</i>	559
f. <i>Information sharing</i>	560
g. <i>Message transport/broadcast</i>	560
19.2. IoT threats from the perspective of cloud security	560
19.3. Exploring cloud service provider IoT offerings	562
19.3.1. <i>AWS IoT</i>	562

a. Kinesis.....	562
b. Amazon Lambda	563
c. Simple storage service (S3)	563
d. CloudWatch	563
e. DynamoDB	564
f. AWS Thing Shadow	564
19.3.2. Microsoft Azure IoT suite	565
19.3.3. Cisco fog computing.....	566
19.3.4. IBM Watson IoT platform.....	566
19.4. Cloud IoT security controls.....	567
19.4.1. Authentication and authorization.....	567
Authentication mechanisms in Amazon AWS.....	568
Authentication mechanisms in Microsoft Azure	568
19.4.2. Software/firmware updates.....	569
19.4.3. End-to-end security recommendations	569
19.4.4. Maintain data integrity	570
19.4.5. Secure bootstrap and enrollment of IoT devices.....	570
19.4.6. Security monitoring.....	570
19.5. An enterprise IoT cloud security architecture	571
19.6. New directions in cloud-enabled IOT computing	573
19.6.1. IoT-enablers of the cloud	573
Software defined networking	574
Data services.....	574
Container for secure development and deployment of IoT environments	574
Microservices	575
19.6.2. Cloud-enabled directions.....	576
On-demand computing and the IoT	576
Cognitive IoT.....	576
Conclusion.....	577
19.7. Questionnaire.....	578
Multiple choice questions.....	578
Answer key	579
Long answer question	579
Short answer questions.....	579
Keywords E F.....	579

References.....	579
Things to check before moving to the upcoming chapter	580
20. Policy-Based Approaches for Informed Consent in IoT.....	581
Structure.....	581
20.1 Informed consent.....	582
20.1.1. <i>Informed consent in Internet of Things</i>	582
20.1.2. <i>Implementation challenges of informed consent in IoT</i>	584
20.2. A policy-based solution for informed consent in IoT.....	585
20.2.1. <i>Policy-based framework</i>	587
<i>Steps for the specification of informed consent (metamodeling)</i>	587
20.2.2. <i>Policy enforcement component</i>	589
20.2.3. <i>Implementation of the SecKit to IoT for informed consent</i>	592
Conclusion.....	594
20.3 Questionnaire.....	595
<i>Multiple choice questions</i>	595
<i>Answer key</i>	596
<i>Long answer question</i>	596
<i>Short answer question</i>	596
Keywords E F.....	596
References.....	596
Things to check before moving to the next chapter.....	596
21. Blockchains for Internet of Things.....	599
Structure.....	599
21.1. Blockchain technology: The introduction	600
21.1.1. <i>Issues with the current banking system and its solutions</i>	600
21.1.2. <i>Architecture of the blockchain</i>	602
<i>Components of block</i>	603
<i>Formation of blockchain</i>	604
21.1.3. <i>Features of blockchain</i>	604
a. <i>Public distributed ledger</i>	604
b. <i>Encryption</i>	605
c. <i>Mining and Proof of Work</i>	607
d. <i>Incentives of mining</i>	609

21.1.4. Use-case of Blockchain technology.....	609
21.2. Crypto-currencies	610
21.2.1. Cryptocurrency examples	612
<i>Bitcoins</i>	612
<i>Ether</i>	612
21.3. Bitcoin P2P network	613
21.4. Distributed consensus.....	614
21.4.1. Types of consensus algorithms	614
<i>a. Proof of work</i>	614
<i>b. Proof of Stake</i>	614
<i>c. Byzantine Fault Tolerance</i>	614
<i>d. Proof of Burn</i>	615
<i>e. Proof of Capacity</i>	615
<i>f. Proof of Elapsed Time</i>	615
21.5. Smart contracts.....	615
21.6. Blockchain wallets	616
21.6.1. Types of Blockchain wallets.....	617
<i>a. Classification based on a private key</i>	617
<i>b. Classification based on application</i>	618
21.7. Altcoins.....	619
21.8. Anonymity	620
Conclusion.....	620
21.9. Questionnaire	622
<i>Multiple choice questions</i>	622
<i>Answer key</i>	623
<i>Long answer questions</i>	623
<i>Short answer questions</i>	623
References.....	623
Keywords E F.....	624
Things to check before moving to the next chapter.....	624
22. Game Theory Foundation	625
Structure.....	625
22.1. Introduction to Game-Theoretic approach	626
22.1.1. Useful terms in Game Theory.....	626

Market game	627
Political game.....	627
Wireless communication game	628
Auction game.....	628
22.1.2. Example 1- Prisoner's Dilemma Game.....	628
Mathematical formulation of the Prisoner's Dilemma Game.....	630
22.2. Best response and Nash equilibrium.....	631
22.2.1. Example 2- market game	634
22.3. Mixed-strategy or randomized-strategy	636
22.3.1. Example 3- Matching pennies game.....	636
22.3.2. Example 4- Paying taxes game	640
Mixed strategy of paying tax game	642
22.4. Repeated games	643
22.4.1. Example 5- Finitely repeated Prisoner's Dilemma Game.....	644
Nash-equilibrium and game table of twice repeated Prisoner's Dilemma Game .	646
22.4.2. Example 6- Finitely repeated games having multiple equilibrium.....	647
22.4.3. Infinitely repeated games.....	649
22.4.4. Example 7- Infinitely repeated Prisoner's Dilemma Game.....	650
Calculus of infinitely repeated triggering strategy.....	651
Calculus of infinitely repeated Prisoner's Dilemma Game.....	651
22.5. Bayesian games.....	652
22.5.1. Example 8- Battle of sexes game	652
Analysis of the Bayesian game.....	654
22.6. Coalitional games	656
22.6.1. Coalitional games with transferable utility.....	657
22.6.1.1. Example 9- Voting game	658
22.6.2. Outcome of coalitional games	658
22.6.3. Classes of coalitional games	659
Relationship between the different classes of games	660
22.6.4. Analyzing coalitional games.....	660
Payoffs division methods	661
The Shapley value	661
The core.....	663
Conclusion.....	664
22.7. Questionnaire	665

<i>Multiple choice questions</i>	665
<i>Answer key</i>	666
<i>Long answer questions</i>	666
<i>Short answer questions</i>	667
References.....	667
Things to check before moving to the next chapter.....	668
23. Security Products	669
Structure.....	670
23.1. Existing IoT security products.....	670
<i>a. AWS IoT device defender</i>	671
<i>b. Microsoft Defender for IoT</i>	671
<i>c. McAfee embedded control</i>	671
<i>d. Entrust IoT security</i>	672
<i>e. IoT security</i>	672
<i>f. Cybeats</i>	672
<i>g. KeyScaler</i>	672
<i>h. Memfault</i>	672
<i>i. Quantum edge</i>	673
<i>j. Spartan</i>	673
23.2. Testbed on security and privacy of IoTs.....	673
<i>a. Smart campus Testbed</i>	674
<i>b. Supersensor testbed</i>	674
<i>c. MakeSense testbed</i>	674
<i>d. INternational Future INdustrial Internet testbed</i>	675
<i>e. SmartSantander testbed</i>	675
<i>f. ASSET testbed</i>	675
<i>g. Stanfords testbed</i>	675
<i>h. Siboni's security testbed for IoT devices</i>	676
23.3. IoT databases and its security.....	676
23.3.1 <i>Threats and challenges of IoT databases with their feasible solutions</i>	677
<i>a. Data privacy and compliance</i>	677
<i>b. Data quality and integrity</i>	678
<i>c. Data security and resilience</i>	678
<i>d. Data governance and ethics</i>	678

<i>e. Data innovation and collaboration</i>	679
<i>f. Data skills and awareness</i>	679
Conclusion.....	679
23.4. Questionnaire.....	680
<i>Multiple choice questions</i>	680
<i>Answer key</i>	681
<i>Long answer question</i>	681
<i>Short answer questions</i>	681
References.....	681
Keywords E F.....	682
Things to check before moving to the next chapter.....	683
Index	685-707

CHAPTER 1

The Internet of Things and its Security Requirements

The Internet of Things is an emerging technology that is spreading rapidly and is making our life easy by changing everything with respect to our utility and lifestyle. For instance, switching on/off the air conditioner while sitting at the office, shutting down the machine with only a click, or auto-halting industrial activities with a change in environment are a few illustrations that explain the utility of IoT in the current world. IoT has persuaded us to live in a world where machines and humans live under the same roof. Apart from providing easy services to users and operators, it is giving an open invitation to criminals and cyber attackers, whose aim is to injure the organization's economic transactions, business transactions, safety, and privacy. Besides damaging the organization; attackers anticipate threats to sensitive data, and to the safety of individual users. Poorly secured IoT devices have been weaponized to assist criminals of domestic abuse that monitor and psychologically distress their victims, particularly women and children.

Considering these facts, it is deduced that securing IoT is of utmost importance, but before diving into the practical aspects of security, the chapter addresses a brief introduction to the Internet of Things.

Structure

In this chapter, we will cover the following topics:

- The Internet of Things and its fundamentals
- The limitations of IoT and the need to secure IoT devices and systems
- The security requirements in IoT architecture and its protocols
- The threats and security in IoT technologies and their applications
- Other IoT-supporting technologies

1.1 Internet of Things - A brief introduction

The Internet of Things is supposed to be the future Internet for the upcoming generation. It is a combination of numerous technologies, which includes sensibility and networking technology, communication technology, service-oriented technology (like Amazon's Alexa, cloud-based IoT voice service), and intelligent information processing technologies (like real-time healthcare processing). In a layman's language, IoT is the network of physical objects that includes sensors, actuators, and microcontrollers, which communicate with each other through low-power protocols via the Internet. The concept of IoT was first proposed in 1999 but still, the standard definition of IoT is yet to originate. As per the standard organizations, the quality-based definitions of IoT are defined as follows:

- According to **International Telecommunication Union (ITU)**, the United Nations Specialized agency for information and communication technologies defines IoT as "A global infrastructure for the information society that enables advanced services by interconnecting things either physically or virtually based on existing and evolving, interoperable information and communication technologies"[1].
- According to IEEE, IoT is defined as "A self-configuring, adaptive, and complex network that interconnects things to the Internet through the use of standard communication protocols. "Things" can be any objects that have sensing/actuation and programming capabilities and can be changed anywhere, anytime, and by anything taking security into consideration [2].

IoT can be used in many ways; it can improve, automate, and control processes with small-scale information like weather forecasting with only one or two parameters. It can help in driving new business models and revenue streams (like manufacturing industries) and provide real-time data to businesses that develop

products and services. There are several domains and environments where IoT has played a remarkable role and has improved the quality of our lives; these include home, health, transportation, industrial automation, energy, agriculture, and many more. The diversifications of these applications are grouped into two categories: consumer IoT and business IoT. Consumer IoT is an IoT where things/objects are personally used by the consumer while in business IoT, sensor-enabled objects are used to provide new insights to businesses, boost their efficiency, and help to make more informed and capable decisions. *Figure 1.1* demonstrates the classification of IoT with help of examples:

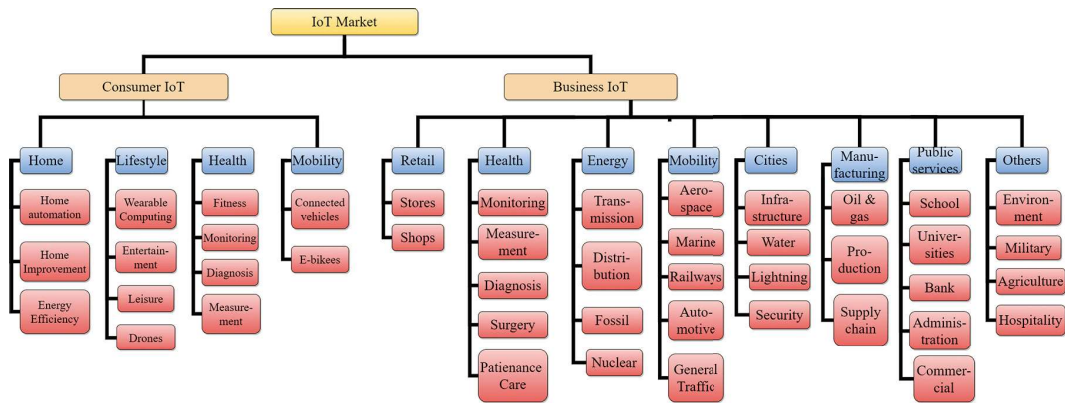


Figure 1.1: Classification of IoT market

1.1.1 Growth trends and market opportunity

As discussed, the applications of IoT are so diversified that it provides a considerable market opportunity to all equipment manufacturers, Internet service providers, and application developers. According to the report 2015 published by McKinsey Global Institute, the global IoT market is expected to roll globally from \$5.5 trillion in 2015 to \$12.6 trillion by 2030[3].

It is the foundation for various organizations that empowers them to enhance the existing processes by creating and monitoring new business models. The growing acquisition of IoT across industries like enterprises, manufacturing, automotive, and healthcare is confidently enhancing the market’s growth. It is encouraging the next industrial revolution of intelligent connectivity, which aims to improve the efficiency of the machines and reduce its downtime.

By 2025, it is estimated that robotization will become part of day-to-day operations and will reach a value of USD 12.3 billion. In addition, M2M traffic flows are expected to constitute 75% of the whole Internet market [4].

Next, healthcare applications are predicted to form the largest impact on economic growth. This has seen a huge rise during the Covid-19 pandemic, where vendors were collaborating with organizations to offer technology-enabled healthcare solutions and help them to overcome the crisis effectively. For instance, *Shanghai Public Health Clinical Center (SPHCC)* has used the California-based connected health startup *VivaLNK's* continuous temperature measuring tool to monitor COVID-19 patients which have therefore reduced the risks of nurses/ doctors and other caregivers being exposed to the threatening virus. According to the IoT healthcare market, the size is expected to grow from USD 72.5 billion in 2020 to USD 188.2 billion by 2025[5].

Not only this, IoT is providing its services to automotive, retail, homes, cities, and so on. The projected market share of these applications by 2030 is illustrated in *Figure 1.2* [3].

It is predicted that the IoT economic value depends on the environment where it is deployed. As per the Global McKinsey report, factory settings, including manufacturing and hospitals, will account for the largest amount of economic growth, around 26% in 2030 followed by human health representing around 10-14% of its economic value in 2030. Please refer to the following figure:

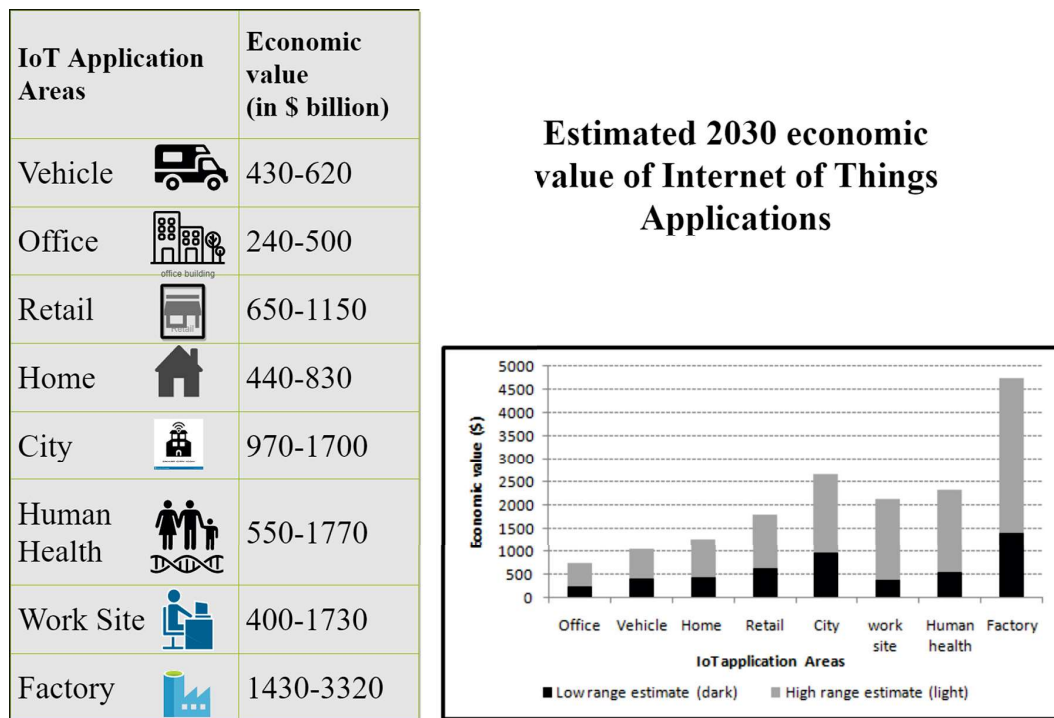


Figure 1.2: IoT Growth Trend

Though all these research and statistics point to a significant growth of the IoT in the near future, related to enterprises and services. However, the transformation of traditional equipment and appliances to smart products would definitely invite threats and vulnerabilities towards it. Securing the IoT and its related services globally requires a security management system to provision their networks with its safety and protection measures. However, before that let's discuss the building blocks of IoT.

1.2 Networking in the IoT device - The framework

The framework and working of IoT can be explained with the help of six building blocks that provide an insight into the meaning and the functionality of the Internet of Things. The elements of IoT include identification, sensing, communication, computation, services, and semantics. Examples of each element are illustrated in *Table 1.1*:

IoT Elements		Examples
Identification	Naming	EPC, uCode
	Addressing	IPv4, IPv6
Sensing		Smart sensors, wearable sensing device, actuators, RFID tags
Communication		RFID, NFC,UWB,Wi-Fi , BLE, LTE,Z-Wave
Computation	Hardware	Aurdino , Raspberry Pi,
	Software	Contiki, Tiny OS, Riot OS, LiteOS
Service		Identity related, information aggregation, Collaborative aware, Ubiquitous
Semantics		RFD,OWL,EXI

Table 1.1: IoT Building Blocks and its Technology

1.2.1 Identification

Identification plays a key role in the Internet of Things where it identifies and matches services as per the demand. Identifiers are used for identification that ensures the correct composition and operation of the system. The process of identification involves naming and addressing schemes.

The naming scheme includes **Electronic Product Codes (EPC)** and ubiquitous codes (uCode) as the object identifier (Object ID). Object ID refers to the instance of the