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/lsyz3qa

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

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:

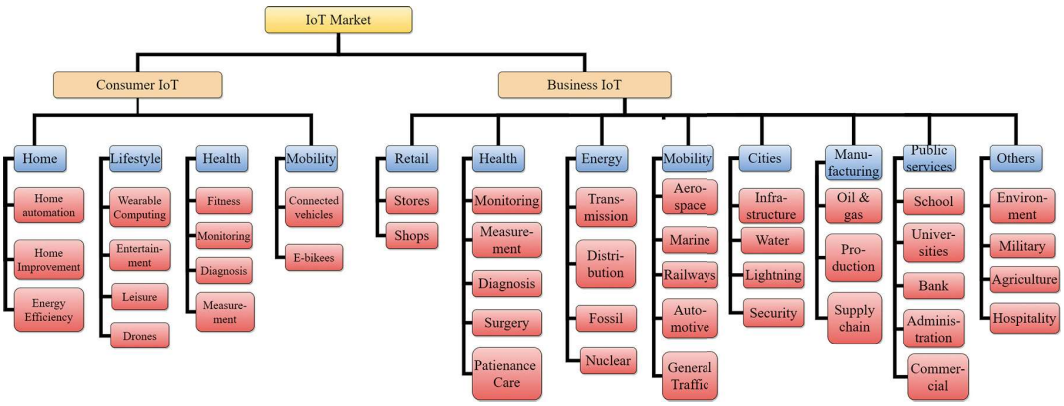

Figure 1.1: *Classification of IoT market*

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:

IoT Application Areas	Economic value (in $ billion)
Vehicle	430-620
Office	240-500
Retail	650-1150
Home	440-830
City	970-1700
Human Health	550-1770
Work Site	400-1730
Factory	1430-3320

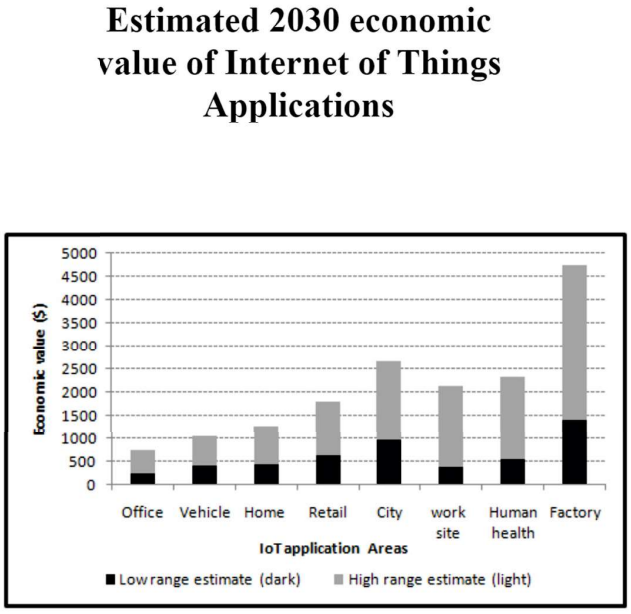

Figure 1.2: *IoT Growth Trend*

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