

The Technical Foundations of IoT

Boris Adryan, Dominik Obermaier, and Paul Fremantle: Artech House; 1st Edition; June 2017; ISBN-13: 978-1-63081-251-5; Hardcover, 453 pages.

Reviewers: Casey Tran and Satyajayant Misra

According to Cisco, the number of connected devices will reach 500 billion by 2030. The myriad devices to be connected to the Internet means that the Internet of Things (IoT) will play a critical role in our future. *The Technical Foundations of IoT*, authored by Adryan, Obermaier, and Fremantle, is intended for professionals interested in research and those who develop and build such IoT end systems. This book equally serves as a reference of context for any reader crossing among the components of IoT whether in software, hardware, networks, or security. The book is divided into eight parts: I, "Physical Principles and Information"; II, "Historical Perspective of the Internet of Things"; III, "Applications of M2M and IoT"; IV, "Architectures of M2M and IoT Solutions"; V, "Hardware"; VI, "Device Communication"; VII, "Software"; and VIII, "Security." In what follows, this review will cover the 29 chapters in these eight parts. Part I deals with the foundational aspects of IoT — hardware. Chapter 1 provides good coverage of the relationship between electricity and electromagnetism, Chapter 2 shows the basic components used to build hardware with a reference to Horowitz and Hill's *The Art of Electronics*. Chapter 3 is a more theoretical complement covering Shannon's "entropy," Turing's "machine," and even analog-to-digital conversion examples to tie this first section together.

Part II contains a short Chapter 4 that opens with a historical background concerning the original intentions of the Advanced Research Projects Agency Network (ARPANET) from a handful of researchers, which grew to a ubiquitous network of billions of devices. The spirit of the initial realization of what is now known as the World Wide Web is properly given and in detail. This part marks the transition to the authors' explicit discussion on IoT from the foundational Part I. The chapter is provoking because it enables a thought exercise in the analogies between Web 2.0 and the upcoming next "boom" of networked technology. The authors historically mention the first "thing" of the Internet starting from a coffee pot web broadcast (The Trojan Room Coffee Pot) to supervisory control and data acquisition systems: machine-to-machine (M2M) and Industrial IoT (IIoT) to the current trend of wearable devices and open source microcontroller boards such as the Arduino Uno and Raspberry Pi.

The purpose of Part III is to explicitly commence the discussion of IoT. It begins by urging the audience to think of IoT "as result of technical evolution." What counts and can be denoted as IoT is given its appropriate definition and requirements apart from merely automation, M2M, IIoT, gadgets, or proprietary IoT. Most importantly, the authors make a point that it must include "interoperability."

Moving forward, Chapter 6, "Applications of M2M and IoT," lists the "five core functionalities of IoT" and gives examples about how these features of IoT may be implemented in IoT ecosystems such as for vehicles, industry, cities, health, and home. To conclude, Chapter 7 ends this part with a discussion of the motivating forces and limitations of IoT. Drivers include examples, such as efficient use of resources, and limitations, including interoperability and standardization, which are discussed in Chapter 25 of Part VII.

Part IV begins the technical aspects of IoT design and organization. In Chapter 8, components for the information flow of IoT devices are stated as analogous to the classical model of information flow in computing (input-processing-output), illustrated by the sensors, gateways/hub devices, and cloud and data

platforms. Chapter 9 introduces a brief overview of network topologies and terms such as LAN, WAN, PAN, BAN, and MAN before the next chapter's presentation on how these relate to IoT and their networking with mesh, gateway, and direct cellular style (Chapter 10). In Chapter 11, the authors conclude this part with considerations of how IoT devices ought to transition into our homes and ubiquitously in our environments.

Part V takes what is learned in Part I into practicality and acquaints the reader with the possible types of hardware pieces and their use. Chapter 12 lists the key steps in planning, prototyping, and testing. Chapter 13 discusses DC and AC power over the Ethernet, and the chemistry and standards of batteries and renewable energy resources. Chapter 14, with sections titled "From Buzzers to Speakers," "From LEDs to Displays," and "From Vibration to Rotation," provides good basic technical examples of how energy can be used to actuate physical outputs. For example, a simple Charlieplexing example is illustrated for an LED display. Chapter 16 ends this section with a focus on the key considerations in microcontroller selection for embedded systems.

Part VI starts with discussions on OSI and TCP/IP models in Chapter 17. Chapter 18 presents encoding schemes such as Manchester and variations of NRZ and device communication without a common clock. Chapter 19 covers the industry standards on the different types of wired and wireless communication models from a simple wired PCI to wireless 5G.

Part VII, "Software," presents Chapter 20 as an introduction to many new and creative software problems in developing for IoT. The authors highlight the challenges of the consistency, availability, and partition tolerance (CAP) theorem, the *Fallacies of Distributed Computing* (Deutsche, 1990), and the challenge of assigning unique identities in growing IoT networks. Chapter 21 focuses on challenges software developers may come across and possible solutions for embedded and constrained devices when dealing with power saving through sleep management and real-time requirements with interrupts. In Chapter 22, the authors present application protocols for IoTs, such as Representational State Transfer (REST), Constrained Application Protocol (COAP), eXtensible Message Presence Protocol (XMPP), Advanced Message Queuing Protocol (AMQP), and Message Queuing Telemetry Transport (MQTT) along with some use cases for each. Chapter 23 contains possible data flows along with a representation of how they may be stored in a back-end software solution for IoT. The chapter also includes discussions on relational database and time-series databases. Chapter 24 discusses how IoT and data mining are used together. It includes discussion of preprocessing at the edge and supervised/unsupervised machine learning techniques. The chapter ends with a discussion of the critical IoT challenge of standardizing ontologies for an "intelligent IoT system."

The last part of the book concludes with security, focusing on the hardware, networking, and cloud systems of IoT networks. This includes information security principles and examples of attacks on connected vehicles in Chapter 26, a good and fun overview of encryption techniques and TLS in Chapter 27 (also with examples); and IoT concerns/challenges on confidentiality, integrity, authenticity, and availability in Chapter 28. Chapter 29 concludes with ways to build and maintain a secure infrastructure.

With the imminence of a greater and more connected world, we are approaching another wave of revolution in connectedness. Just as the use of the Internet came as a surprise, IoT will no doubt be the same in how it affects and presents novel ways in how we interact with each other, our machines, and our world. This book could be viewed as presenting the reader with the technical "bones" of IoT so that he/she may lay flesh on them by discerning how and why the pieces ought to fit together.