Preface

Technology is becoming embedded in nearly everything in our lives. Just look around you and you will see how the Internet has completely affected many aspects of our existence. Virtually anything you desire can be ordered instantly, at a push of a button, and delivered to your door in a matter of days if not minutes. We all see the impact of smartphones, smart appliances, and smart cars to cite a few.

Today, manufacturers are installing tiny sensors in effectively every device they make and utilizing the Internet and cloud computing to connect such devices to data centers capturing critical information. By connecting things with cloud technology and leveraging mobility, desired data is captured and shared at any location and any time. The data is then analyzed to provide businesses and consumers with value that was unattainable just a decade or less ago.

Up to the minute information is provided about the states and locations of services. Further, businesses use the sensors to collect mission critical data throughout their entire business process, allowing them to gain real-time visibility into the location, motion and state of assets, people and transactions and enabling them to make smarter decisions.

As more objects become embedded with sensors and the ability to communicate, new business models become possible across the industry. These models offer to improve business processes, reduce costs and risks, and more importantly create huge business opportunities in a way that changes the face and the pace of business. Experts agree that the Internet of Things will revolutionize businesses beyond recognition in the decades to come.

At the core of the success of the Internet, and one of its foundational principles, is the presence of a common protocol layer, the IP layer, which provides normalization of a plethora of applications (e.g., e-mail, web, voice, and video) over numerous transport media (e.g., Ethernet, Wi-fi, and cellular). Graphically, this can be rendered as an hourglass with IP in the middle: IP being the thin waist of this proverbial hourglass. This model has served well, especially since the Internet, over the past three decades, has been primarily concerned with enabling connectivity: interconnecting networks across the globe. As the Internet evolves into the Internet of Things, the focus shifts from connectivity to data. The Internet of Things is

primarily about data and gaining actionable insights from that data, as discussed above. From a technology perspective, this can be achieved with the availability of networking protocols that meet the requirements and satisfy the constraints of new Internet of Things devices, and more importantly with the availability of standard interfaces and mechanisms for application services including data access, storage, analysis, and management. How does this translate to the proverbial hourglass? At the very least, a second thin waist is required which provides a common normalization layer for application services.

The road to a standards-based Internet of Things is well underway. The industry has made significant strides toward converging on the Internet protocol as the common basis. Multiple standards have been defined or are in the process of being defined to address the requirements of interconnecting "Things" to the Internet. However, many gaps remain especially with respect to application interoperability, common programmable interfaces, and data semantics. How the Internet of Things will bend and mold the IP hourglass in the decades to come will certainly be fascinating to witness. We, as engineers, developers, researchers, business leaders, consumers, and human beings are in the vortex of this transformation.

In this book, we choose to introduce the Internet of Things (IoT) concepts and framework in the earlier chapters and avoid painting examples that tie the concepts to a specific industry or to a certain system. In later chapters, we provide examples and use cases that tie the IoT concepts and framework presented in the earlier chapters to industry verticals.

Therefore, we concentrate on the core concepts of IoT and try to identify the major gaps that need to be addressed to take IoT from the hype stage to concrete reality. We also focus on equipping the reader with the basic knowledge needed to comprehend the vast world of IoT and to apply that knowledge in developing verticals and solutions from the ground up, rather than providing solutions to specific problems. In addition, we present detailed examples that illustrate the implementation and practical application of abstract concepts. Finally, we provide detailed business and engineering problems with answer guides at the end of each chapter.

The following provides a chapter by chapter breakdown of this book's material.

Chapter 1 introduces the foundation of IoT and formulates a comprehensive definition. This chapter presents a framework to monitor and control things from anywhere in the world and provides business justifications on why such monitoring and control of things are important to businesses and enterprises. It then introduces the 12 factors that make IoT a present reality.

The 12 factors consist of (1) the current convergence of IT and OT, (2) the astonishing introduction of creative Internet-based businesses with emphasis on Uber, Airbnb, Square, Amazon, Tesla, and the self-driving cars, (3) mobile device explosion, (4) social network explosion, (5) analytics at the edge, (6) cloud computing and virtualization, (7) technology explosion, (8) digital convergence/transformation, (9) enhanced user interfaces, (10) fast rate of IoT technology adoption (five times more than electricity and telephony), (11) the rise

of security requirements and (12) the none-stop Moore's law. The last section of this chapter presents a detailed history of the Internet.

Chapter 2 describes the "Internet" in the "Internet of Things". It starts with a summary of the well-known open system interconnection (OSI) model layers. It then describes the TCP/IP Model, which is the basis for the Internet. The TCP/IP has two big advantages in comparison with earlier network protocols: reliability and flexibility to expand. The TCP/IP was designed for the US Army addressing the reliability requirement (resist breakdowns of communication lines in times of war). The remarkable growth of Internet applications can be attributed to this reliable expandable model.

Chapter 2 then compares IP version 4 with IP version 6 by illustrating the limitations of IPv4, especially for the expected growth to 26.3 billion devices with IoT. IPv4 has room for about 4.3 billion addresses, whereas IPv6, with a 128-bit address space, has room for 2^{128}, or 340 trillion trillion trillion addresses. Finally, detailed description of IoT network level routing is described and compared with classical routing protocols. This chapter finally discusses the IoT network level routing that incudes interior and exterior routing protocols.

Chapter 3 defines the "Things" in IoT and describes the key requirements for things to be able to communicate over the Internet: sensing and addressing. Sensing is essential to identify and collect key parameters for analysis and addressing is necessary to uniquely identify things over the Internet. While sensors are very crucial in collecting key information to monitor and diagnose the "Things", they typically lack the ability to control or repair such "Things" when action is required. This chapter answers the question: Why spend money to sense "Things" if they cannot be controlled? It illustrates that actuators are used to address this important question in IoT. With this in mind, the key requirements for "Things" in IoT now consist of the following: sensing, actuating, and unique identification. Finally, this chapter identifies the main sensing technologies that include physical sensors, RFID, and video tracking and discusses the advantages and disadvantages of these solutions.

Chapter 4 discusses the requirements of IoT which impact networking protocols. It first introduces the concept of constrained devices, which are expected to comprise a significant fraction of new devices being connected to the Internet with IoT. These are devices with limited compute and power capabilities; hence they impose special design considerations on networking protocols which were traditionally built for powerful mains connected computers. This chapter then presents the impact of IoT's massive scalability on device addressing in light of IPv4 address exhaustion, on credentials management and how it needs to move toward a low-touch lightweight model, on network control plane which scales as a function of the number of nodes in the network, and on the wireless spectrum that the billions of wireless IoT devices will contend for.

After that, this chapter goes into the requirements for determinism in network latency and jitter as mandated by real-time control applications in IoT, such as factory automation and vehicle control systems. This is followed by an overview of the security requirements brought forward by IoT. Then, this chapter turns into

the requirements for application interoperability with focus on the need for standard abstractions and application programmatic interfaces (APIs) for application, device, and data management, as well as the need for semantic interoperability to ensure that all IoT entities can interpret data unambiguously.

Chapter 5 defines the IoT protocol stack and compares it to the existing Internet protocol stack. It provides a layer-by-layer walkthrough of that stack, and, for each such layer, discusses the challenges brought forward by the IoT requirements of the previous chapter, the industry progress made to address those challenges, and the remaining gaps that require future work.

Starting with the link layer, this chapter discusses the impact of constrained device characteristics, deterministic traffic characteristics, wireless access characteristics, and massive scalability on this layer. It then covers the industry response to these challenges in the following standards: IEEE 802.15.4, TCSH, IEEE 802.11ah, and time sensitive networking (TSN). Then shifting to the Internet layer, this chapter discusses the challenges in low power and lossy networks (LLNs) and the industry work on 6LowPAN, RPL, and 6TiSCH. After that, this chapter discusses the application protocols layer, focusing on the characteristics and attributes of the protocols in this layer as they pertain to IoT, and highlighting, where applicable, the requirements and challenges that IoT applications impose on these protocols. This chapter also provides a survey and comparison of a subset of the multitude of available protocols, including CoAP, MQTT, and AMQP to name a few. Finally, in the application services layer, this chapter covers the motivation and drivers for this new layer of the protocol stack as well as the work in ETSI M2M and oneM2M on defining standard application middleware services.

Chapter 6 defines fog computing, a platform for integrated compute, storage, and network services that is highly distributed and virtualized. This platform is typically located at the network edge. This chapter discusses the main drivers for fog: data deluge, rapid mobility, reliable control and finally data management and analytics. It describes the characteristics of Fog, which uniquely distinguish it from cloud computing.

This chapter then focuses on the prerequisites and enabling technologies for fog computing: virtualization technologies such as virtual machines and containers, network mobility solutions including EVPN and LISP, fog orchestration solutions to manage topology, things connectivity and provide network performance guarantees, and last but not least data management solutions that support data in motion and distributed real-time search. This chapter concludes with the various gaps that remain to be addressed in orchestration, security, and programming models.

Chapter 7 introduces the IoT service platform, which is considered to be the cornerstone of successful IoT solutions. It illustrates that the service platform is responsible for many of the most challenging and complex tasks of the solution. It automates the ability to deploy, configure, troubleshoot, secure, manage, and monitor IoT entities, ranging from sensors to applications, in terms of firmware installation, patching, debugging, and monitoring to name just a few. The service platform also provides the necessary functions for data management and analytics,

temporary caching, permanent storage, data normalization, policy-based access control, and exposure.

Given the complexity of the services platform in IoT, this chapter groups the core capabilities into 11 main areas: platform, discovery & registration, communication (delivery handling), data management & repository, firmware, topology management, group management, billing and accounting, cloud service integration, API and finally element manager addressing configuration management, fault management, performance management, and security management across all IoT entities.

Chapter 8 focuses on defining the key IoT security and privacy requirements. Ignoring security and privacy will not only limit the applicability of IoT but will also have serious results given that all the physical objects in our surroundings will be connected to the network. In this chapter, the IoT security challenges and IoT security requirements are identified. A three-domain IoT architecture is considered in the analysis where we analyze the attacks targeting the cloud domain, the fog domain, and the sensing domain. The analysis describes how the different attacks at each domain work and what defensive countermeasures can be applied to prevent, detect, or mitigate those attacks.

This chapter ends by providing some future directions for IoT security and privacy that include fog domain security, collaborative defense, lightweight cryptography, lightweight network security protocols and digital forensics.

Chapter 9 describes IoT vertical markets and connected ecosystems. It first introduces the top IoT verticals that include agriculture & farming, energy, enterprise, finance, health care, industrial, retail, and transportation. Such verticals include a plethora of sensors producing a wealth of new information about device status, location, behavior, usage, service configuration, and performance. This chapter then presents a new business model driven mainly by the new information, and illustrates the new business benefits to the companies that manufacture, support, and service IoT products, especially in terms of customer satisfaction. It then presents the key requirements to deliver "Anything as a Service" in IoT followed by a specific use case.

Finally, Chap. 9 combines IoT verticals with the new business model and identifies opportunities for innovative partnerships. It shows the importance of ecosystem partnerships given the fact that no single vendor would be able to address all the business requirements.

Chapter 10 provides an overview of the IoT standardization landscape and a glimpse into the main standards defining organizations involved in IoT as well as a snapshot of the projects that they are undertaking. It highlights the ongoing convergence toward the Internet protocol as the normalizing layer for IoT. This chapter covers the following industry organizations: IEEE, IETF, ITU, IPSO Alliance, OCF, IIC, ETSI, oneM2M, AllSeen Alliance, Thread Group, ZigBee Alliance, TIA, Z-Wave Alliance, OASIS, and LoRa Alliance. This chapter concludes with a summary of the gaps and provides a scorecard of the industry progress to date.

Chapter 11 defines open source in the computer industry and compares the development cycles of open source and closed source projects. It discusses the

drivers to open source from the perspective of the consumers of open source projects as well as contributors of these projects. This chapter then goes into discussing the interplay between open source and industry standards, and stresses the tighter collaboration ensuing among them.

This chapter then provides a tour of open source activities in IoT ranging from hardware and operating systems to IoT service platforms.

Finally Appendix A presents a comprehensive IoT glossary that includes the definitions of over 1200 terms using information from various sources that include key standards and latest research.

San Jose, USA — Ammar Rayes
Vancouver, Canada — Samer Salam

http://www.springer.com/978-3-319-44858-9

Internet of Things From Hype to Reality
The Road to Digitization
Rayes, A.; Salam, S.
2017, XXVIII, 328 p. 109 illus., 105 illus. in color.,
Hardcover
ISBN: 978-3-319-44858-9