Internet of Things From Hype to Reality

Ammar Rayes • Samer Salam

Internet of Things From Hype to Reality

The Road to Digitization

Second Edition

Springer

Ammar Rayes
San Jose, CA, USA

Samer Salam
Beirut, Lebanon

ISBN 978-3-319-99515-1 ISBN 978-3-319-99516-8 (eBook)
https://doi.org/10.1007/978-3-319-99516-8

Library of Congress Control Number: 2018955510

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To invent, you need a good imagination and a pile of junk.

– Thomas A. Edison

To invent, you need the Internet, communication, good imagination and a pile of things.

– Ammar Rayes

Creativity is just connecting things. When you ask creative people how they did something, they feel a little guilty because they didn't really do it, they just saw something. It seemed obvious to them after a while. That's because they were able to connect experiences they've had and synthesize new things.

– Steve Jobs

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.

– Samer Salam

Foreword 1

In California, just a few months after two people stepped foot on the Moon for the first time, two computers began sending messages to each other using protocols designed to make it easy for other computers to connect and join the party (Leiner et al. 2009). On October 29, 1969, a computer in Leonard Kleinrock's lab at UCLA and a computer in Doug Engelbart's lab at SRI forged the first two nodes in what would become known as the Internet. Vint Cerf and two colleagues coined the term Internet as a shortened version of internetworking in December 1974. It did not take long for more computers and their peripherals, as well as more networks of computers, and even industrial equipment to connect and begin communicating messages, including sharing sensor data and remote control instructions. In early 1982, a soda machine at CMU became arguably the first Internet-connected appliance, announced by a broadly distributed email that shared its instrumented and interconnected story with the world. By 1991, it was clear to Mark Weiser that more and more things would someday have embedded computers, including mobile phones, cars, even door knobs, and someday even clothing (Weiser 1991). Today, spacecraft are Internet-connected devices on missions exploring other planets and heading to deep space beyond our solar system. Courtesy of NASA engineers, some are even sending tweets to millions of followers here on Earth about their progress.

The Internet of Things (also known as the Internet of Everything) continues to grow rapidly today. In fact, the Internet of Things (IoT) forms the basis of what has become known as the Fourth Industrial Revolution and digital transformation of business and society (Lee et al. 2014). The first industrial revolution was the steam engine as the focal machine, the second revolution included the machines of mass production, the third revolution was based on machines with embedded computers, and the fourth revolution (today) interconnected machines and things, including information about the materials and energy usage flowing into and out of a globally interconnected cyberphysical system of systems. The level of instrumentation and interconnection is laying the infrastructure for more intelligence, including cognitive computing to be incorporated.

Why does the IoT continue to grow so rapidly? What are the business and societal drivers of its rapid growth? How does IoT relate to the Internet, what types of things make up the IoT, and what are the fundamental and new protocols being used today? How do the specific layers of the IoT protocol stack related to each other? What is the fog layer? What is the Services Platform layer? How are the security and data privacy challenges being resolved? What are the economic and business consequences of IoT, and what new ecosystems are forming? What are the most important open standards associated with IoT, and how are they evolving?

In this introductory IoT textbook, Dr. Ammar Rayes (Cisco, Distinguished Engineer) and Samer Salam (Cisco, Principal Engineer) guide the reader through answers to the above questions. Faculty will find well-crafted questions and answers at the end of each chapter, suitable for review and in classroom discussion topics. In addition, the material in the book can be used by engineers and technical leaders looking to gain a deep technical understanding of IoT as well as by managers and business leaders looking to gain a competitive edge and understand innovation opportunities for the future. Information systems departments based in schools of management, engineering, or computer science will find the approach used in this textbook suitable as either a primary or secondary source of course material.

In closing, and on a personal note, it has been a pleasure to call Dr. Ammar Rayes a colleague and friend for nearly a decade. He has given generously of his time as founding President of the International Society of Service Innovation Professionals (ISSIP.org), a professional association dedicated to helping multidisciplinary students, faculty, practitioners, policy-makers, and others learn about service innovation methods for business and societal applications. Ammar is one of those rare technical leaders who contributes in business, academics, and professional association contexts. My thanks to Ammar and Samer for this excellent introduction to Internet of Things, as it is one more in a line of their contributions that will help inspire the next generation of innovators to learn, develop professionally, and make their own significant contributions.

IBM Jim Spohrer
San Jose, CA, USA

References

J. Lee, H.A. Kao, S. Yang, Service innovation and smart analytics for industry 4.0 and big data environment. Procedia CIRP. **16**, 3–8 (2014)

B.M. Leiner, V.G. Cerf, D.D. Clark, R.E. Kahn, L. Kleinrock, D.C. Lynch, J. Postel, L.G. Roberts, S. Wolff, A brief history of the internet. ACM SIGCOMM Comput. Commun. Rev. **39**(5), 22–31 (2009)

M. Weiser, The computer for the 21st century. Scientific American. **265**(3), 94–104 (1991)

Foreword 2

The Internet of Things (IoT) has been many years in the making. Indeed, the concept of using sensor devices to collect data and then transfer it to applications across a network has been around for several decades. For example, legacy programmable logic controller (PLC) systems already provide data collection and remote actuator control using specialized networking protocols and topologies. Even though these setups have limited footprints and are rather costly, they are still widely used in many industrial settings. Meanwhile, academic researchers have also studied the use of networked sensors for various applications in recent years.

However, continuing market shifts and technology trends in the past decade have dramatically altered the value proposition of interconnected sensors and actuators. Namely, the combination of low-cost hardware and high-speed networking technologies—both wired and wireless—have enabled a new generation of compact sensor devices with ubiquitous connectivity across the wider Internet. These systems are facilitating real-time data collection/sharing and providing unprecedented visibility and control of assets, personnel, operations, and processes. The further use of cloud-based computing/storage facilities is introducing even more advanced data analysis capabilities, ushering in a new era of intelligent decision-making, control, and automation. Broadly, these new paradigms are termed as the *Internet of Things* (IoT).

Indeed there is considerable excitement, perhaps even hype, associated with the IoT. However, as technological advances and business drivers start to align here, related paradigms are clearly poised at an inflection point of growth. For example, a wide range of business and mission-critical IoT systems are already being deployed in diverse market sectors, i.e., including defense, energy, transportation, civil infrastructure, healthcare, home automation/security, agriculture, etc. New cloud and fog computing services are also emerging to deliver actionable insights for improving business productivity and reducing cost/risk. As these new business models start to take hold, the projected IoT market opportunity is huge, widely projected to be in the trillions of dollars in the coming decade.

In light of the above, this text presents a very timely and comprehensive look at the IoT space. The writing starts by introducing some important definitions and reviewing the key market forces driving IoT technology growth. The fundamental IoT building blocks are then presented, including networking systems and sensor technologies. Most notably, IoT-specific networking challenges and requirements are first overviewed, including device constraints, identification, performance determinism, security, and interoperability. Emerging, streamlined IoT protocol stacks are then detailed, covering topics such as layering, routing, and addressing. The main types of sensing technologies are also discussed here along with actuator control devices. Note that the initial part of this text focuses on core IoT concepts and frameworks, leaving more industry and application-specific treatments to later.

The text then addresses broader topics relating to intelligent data management and control for IoT. Namely, the distributed fog computing platform is outlined first, including market drivers, prerequisites, and enabling technologies within the context of IoT. The crucial notion of an IoT service platform is also presented, touching upon issues such as deployment, configuration, monitoring, and troubleshooting. The writing also outlines critical security and privacy concerns relating to IoT, i.e., by categorizing a range of threat scenarios and highlighting effective countermeasures and best practices.

Finally, the latter part of the text progresses into some more business-related aspects of IoT technology. This includes a critical look at emerging vertical markets and their interconnected ecosystems and partnerships, i.e., across sectors such as energy, industrial, retail, transportation, finance, healthcare, and agriculture. Sample business cases are also presented to clearly tie in industry verticals with earlier generalized IoT concepts and frameworks. Finally, the critical role and efforts of IoT standardization organizations is reviewed along with a look at some important open source initiatives.

Overall, both authors are practicing engineers in the networking industry and actively involved in research, technology development, standards, and business marketing initiatives. As result they bring together wide-ranging and in-depth field experience across many diverse areas, including network management, data security, intelligent services, software systems, data analytics, and machine learning, etc. They are also widely published in the research literature and have contributed many patent inventions and standardization drafts. Hence this team is uniquely qualified to write on this subject.

In summary, this text provides a very compelling study of the IoT space and achieves a very good balance between engineering/technology focus and business context. As such, it is highly recommended for anyone interested in this rapidly expanding field and will have broad appeal to a wide cross section of readers, i.e., including engineering professionals, business analysts, university students, and professors. Moreover, each chapter comes with a comprehensive, well-defined set of questions to allow readers to test their knowledge on the subject matter (and answer guides are also available for approved instructors). As such, this writing also provides an ideal set of materials for new IoT-focused graduate courses in engineering and business.

Department of Electrical Engineering
& Florida Center for Cybersecurity (FC2)
University of South Florida,
Tampa, FL, USA

Nasir Ghani

Preface

Technology is becoming embedded in nearly everything in our lives. Just look around you and you will see how the Internet has 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 hours. We all see the impact of smart phones, 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., email, web, voice, video) over numerous transport media (e.g., Ethernet, Wi-Fi, 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. The 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 is 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 nonstop 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 protocol has two big advantages in comparison with earlier network protocols: reliability and flexibility to expand. The TCP/IP protocol 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. It is mentioned that routing tables are used in routers to send and receive packets. Another key feature of TCP/IP routing is the fact that IP packets travel through an internetwork one router hop at a time, and thus the entire route is not known at the beginning of the journey. The chapter finally discusses the IoT network level routing that includes Interior and Exterior Routing Protocols.

Chapter 3 defines the "Things" in IoT and describes the key requirements for things to be able 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. The 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 sensing, actuating, and unique identification. Finally, the 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. The 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, the 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, the 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, the 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, LoRaWAN and Time-Sensitive Networking (TSN). Then, shifting to the Internet layer, the chapter discusses the challenges in Low Power and Lossy Networks (LLNs) and the industry work on 6LowPAN, RPL, and 6TiSCH. After that, the 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. The 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, the 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. The 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.

The 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. The 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, the chapter groups the core capabilities into 11 main areas: Platform Manager, Discovery and Registration Manager, Communication (Delivery Handling) Manager, Data Management and Repository, Firmware Manager, Topology Management, Group Management, Billing and Accounting Manager, Cloud Service Integration Function/Manager, API Manager, 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 on the different aspects of our lives, especially 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.

The 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 and farming, energy, enterprise, finance, healthcare, 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. The 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 discusses blockchain in IoT. It briefly introduces the birth of blockchain technology and its use in Bitcoin. In addition, it describes Bitcoin as an application of blockchain and distinguishes blockchain as a key technology, one that has various use cases outside of Bitcoin. Next, it dives into how blockchains work and outlines the features of the technology; these features include consensus algorithms, cryptography, decentralization, transparency, trust, and smart contracts. The chapter then introduces how blockchain may impact notable use cases in IoT including healthcare, energy management, and supply chain management. It reviews the advantages and disadvantages of blockchain technology and highlights security considerations within blockchain and IoT.

Chapter 11 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. The 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. The chapter concludes with a summary of the gaps and provides a scorecard of the industry progress to date.

Chapter 12 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. The chapter then goes into discussing the interplay between open source and industry standards and stresses the tighter collaboration ensuing among them.

The 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. Appendix B presents examples of IoT Projects.

San Jose, CA, USA — Ammar Rayes
Beirut, Lebanon — Samer Salam

Acknowledgments

We realize that the completion of this book could not have been possible without the support of many people whose names go far beyond the list that we can recognize here. Their effort is sincerely appreciated, and support is gratefully recognized. With that in heart and mind, we would like to express our appreciation and acknowledgment particularly to the following.

First, we would like to express our gratitude to members of the Cisco executive team for their support. In particular, thanks to Rich Plane, head of Cisco's Customer Experience Technology Office; James Mobley, VP/GM of Emerging Technologies & Innovation for Cisco's Customer Experience; and Pradeep Kathail, Chief Network Architect of the Enterprise Networking Business, for their support in the planning and preparation of this book.

We also would like to express our gratefulness to Dr. Jim Spohrer of IBM Research and Professor Nasir Ghani of the University of South Florida for taking the time to write comprehensive forewords. We are very grateful to Alumni Distinguished Graduate Professor and IEEE Fellow, Harry Perros of North Carolina State University, and Dr. Alex Clemn for peer-reviewing the book proposal. Special thanks to Carlos Davila and Jacob Tarnow for co-authoring Chap. 10. Special thanks also go to Dr. Mehiar Dabbagh and Lionel Florit for their contributions in Chaps. 8 and 11, respectively.

Ammar is ceaselessly thankful to his wife Rana and his children Raneem, Merna, Tina, and Sami for their love and patience during the long process of writing this book.

Samer would like to thank his parents, to whom he is eternally grateful, his wife Zeina and children Kynda, Malek, and Ziyad for their love, support, and encouragement that made this book possible. Last but not least, he would like to thank Samir, especially for his help on the use cases and his sense of humor.

Disclaimer

The recommendations and opinions expressed in this book are those of the authors and contributors and do not necessarily represent those of Cisco Systems.

Contents

Authors Biography

Ammar Rayes is a Distinguished Engineer at Cisco Customer Experience Technology Office. His current works include IoT, network analytics, machine learning, and data security. Previously at Cisco, he led solution teams focusing on mobile wireless, network management NMS/OSS, and Metro Ethernet. Prior to join Cisco, he was the Director of Traffic Engineering at Bellcore (formally Bell Labs).

Ammar has authored 3 books, over 100 publications in refereed journals and conferences on advances in software and networking related technologies, and over 30 patents.

Ammar is the Founding President of the International Society of Service Innovation Professionals (www.issip.org), Adjunct Professor at SJSU, Editor in Chief of *Advances in Internet of Things* journal, and Board Member on Transactions on Industrial Networks and Intelligent Systems. He has served as Associate Editor of *ACM Transactions on Internet Technology* and *Wireless Communications and Mobile Computing* journals, Guest Editor of multiple journals and several *IEEE Communications Magazine* issues, Co-chaired the Frontiers in Service Conference and appeared as Keynote Speaker at multiple IEEE and industry conferences.

At Cisco, Ammar is the Founding Chair of Cisco Services Research board and program and the Founding Chair of Cisco Services Patent council. He received Cisco Chairman's Choice Award for IoT Excellent Innovation & Execution in 2013.

He received his BS and MS degrees in EE from the University of Illinois at Urbana—Champaign, IL, USA, and his PhD degree in EE from Washington University in St. Louis, MO, USA, where he received the Outstanding Graduate Student Award in Telecommunications.

Samer Salam is a Principal Engineer at Cisco Systems. He focuses on the system and software architecture for networking products in addition to technology incubation. His work covers the areas of semantic technologies, machine reasoning, IoT data management and analytics, machine to machine communication, as well as next-generation Layer 2 networking solutions and protocols.

Previously at Cisco, he held multiple technical leadership and software development positions working on Layer 2 VPNs, Carrier/Metro Ethernet services, OAM, network resiliency, system scalability, software quality, multiservice edge, broadband, MPLS, and dial solutions.

He holds over 75 US and international patents, is author of more than 20 IETF drafts and RFCs, and has authored several articles in telecommunications industry journals. He is also a speaker at CiscoLive and blogs on networking technology at http://blogs.cisco.com/author/samersalam.

He holds an MS degree in Computer Engineering from the University of Southern California in Los Angeles and a BE degree in Computer and Communications Engineering, with Distinction, from the American University of Beirut, where he received the Faculty of Engineering and Architecture Dean's Award for Creative Achievement.