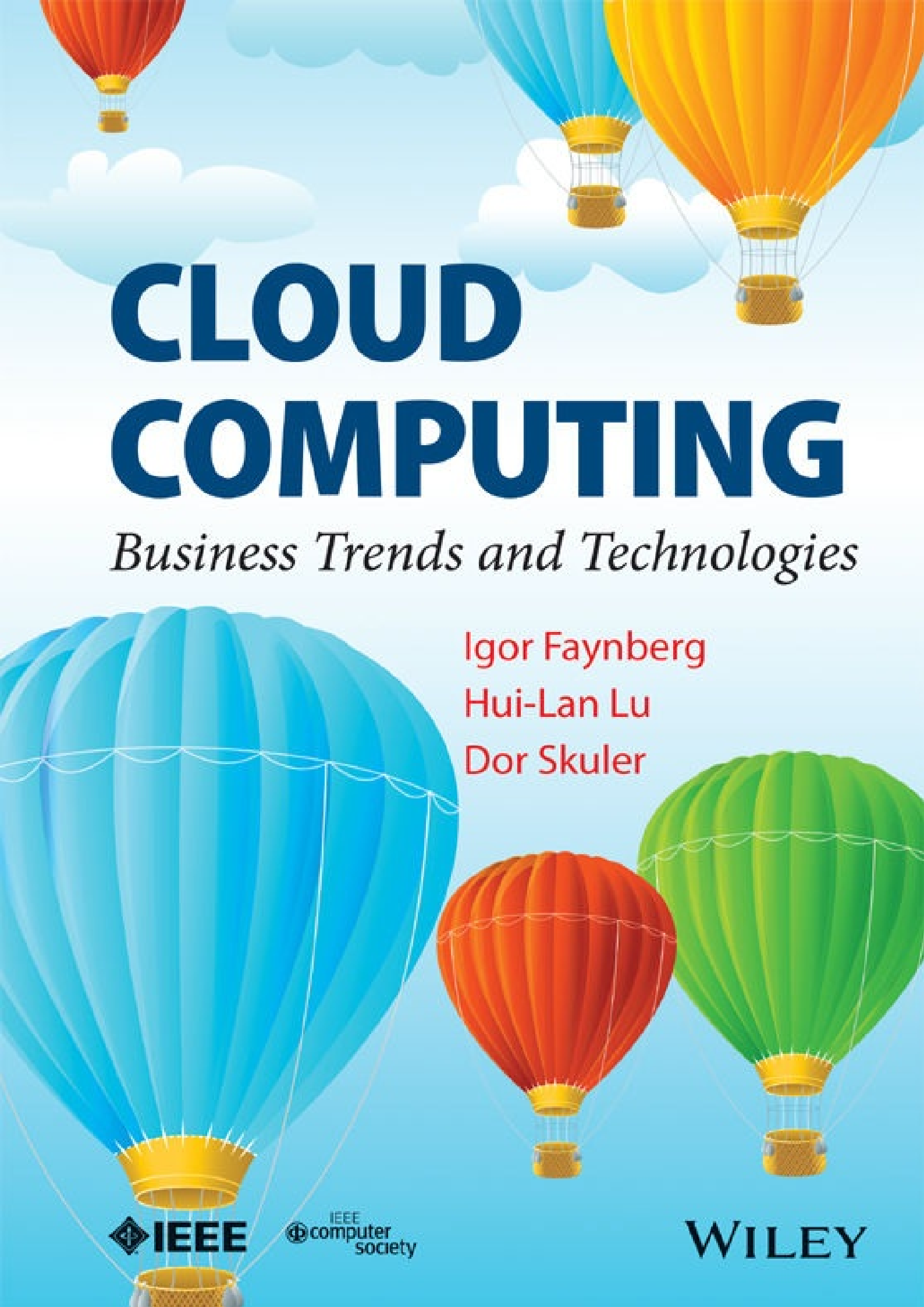
CLOUD
COMPUTING
Business Trends and Technologies
Igor Faynberg
Hui-Lan Lu
Dor Skuler
IEEE
IEEE computer society
WILEY

CLOUD COMPUTING

BUSINESS TRENDS AND TECHNOLOGIES

Igor Faynberg
Hui-Lan Lu
Dor Skuler

WILEY

This edition first published 2016

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

Library of Congress Cataloging-in-Publication Data

Faynberg, Igor.
Cloud computing : business trends and technologies / Igor Faynberg, Hui-Lan Lu, Dor Skuler, Alacatel-Lucent.
pages cm
Includes bibliographical references and index.
ISBN 978-1-118-50121-4 (cloth)

1. Cloud computing. I. Lu, Hui-Lan. II. Skuler, Dor. III. Title.
QA76.585.F38 2016
004.67′82—dc23

2015022953

A catalogue record for this book is available from the British Library.

ISBN: 9781118501214

Contents

List of Illustrations

About the Authors

This book was written while the authors worked in the *CloudBand* Business Unit at Alcatel-Lucent. *CloudBand,* founded by Dor Skuler, is a market-leading platform for Network Functions Virtualization (NFV).

Igor Faynberg, Adjunct Professor in the Computer Science Department of Stevens Institute of Technology, is a Bell Labs Fellow. At the time of writing this book, he was a senior architect in charge of NFV security, reporting to the Chief Technology Officer of *CloudBand*.

Previous to that he had held various staff and managerial positions in Bell Labs and Alcatel-Lucent business units. In his Bell Labs career, he has influenced the development of several software technologies—from mathematical programming to Intelligent Network and Internet/PSTN convergence to virtualization. He has contributed to and held various leadership positions in the Internet Engineering Task Force (IETF), International Telecommunication Union (ITU), and European Telecommunication Standardization Institute (ETSI), where he presently serves as Chairman of the ETSI NFV Security working group. He has served on technical committees of several IEEE conferences, and he holds numerous patents for the inventions related to technologies that he had developed.

Igor has also co-authored two books and numerous refereed papers. He holds a Mathematics Diploma from Kharkov University, Ukraine, and MS and PhD degrees in Computer and Information Science from the University of Pennsylvania.

Hui-Lan Lu is a Bell Labs Fellow at Alcatel-Lucent, where she has conducted research and development in various areas, including mathematical programming, service creation, IP multimedia communication, quality of service in converged networks, and security.

She has been also involved in strategic standards efforts in the IETF, ITU, and ETSI. More recently, she has served as Rapporteur for the ETSI NFV case study of *OpenStack* security and Vice Chairman of ITU-T SG 13 (the lead study group on Cloud Computing and future networks).

Hui-Lan has co-authored a book on converged networks and services, and numerous refereed papers. She holds a PhD degree in physics from Yale University in New Haven and has over 40 patents.

Dor Skuler formerly served as Senior Vice President and General Manager of the *CloudBand* Business Unit at Alcatel-Lucent, which he founded. Prior to this role, Dor served as Vice President of Strategy and Head of Corporate Development for Alcatel-Lucent in its corporate headquarters in Paris. Previously Dor had held entrepreneurial roles such as General Manager of Mobile Security, a new venture in Alcatel-Lucent's Bell Labs and Enterprise Business Divisions.

Before joining Alcatel-Lucent, Dor served as Vice-President of Business

Development and Marketing at *Safend*, an endpoint security company. Dor also founded and served as President of *Zing Interactive Media*, a venture-backed startup company in the field of mobile interactive media.

Dor holds a Master's of Science in Marketing and an MBA in International Business. Dor was selected in Global Telecom Business' “40 under 40” list in 2009, 2011 and 2013 and is often invited to speak in industry events and is interviewed by the global press.

Acknowledgments

A book of this scope and size could not have been written without help from many people. We acknowledge much stimulation that came from early discussions with Markus Hofmann who headed the Bell Labs research effort in the Cloud. We have had incisive discussions on various topics of networking with Mark Clougherty, Vijay Gurbani, and Dimitri Stiliadis.

We have been much influenced and supported by David Amzallag (then CTO of *CloudBand*), particularly on the topic of operations and management.

Our first steps in addressing Cloud security were made together with Doug Varney, Jack Kozik, and Herbert Ristock (now with *Genesys*). We owe much of our understanding of the subject to our *CloudBand* colleagues—Ranny Haibi, Chris Deloddere, Mark Hooper, and Avi Vachnis. Sivan Barzilay has reviewed Chapter 7, to which she has contributed a figure; we also owe to her our understanding of TOSCA.

Peter Busschbach has reviewed Chapter 3 and provided insightful comments.

A significant impetus for this book came from teaching, and the book is intended to be an assigned text in a graduate course on Cloud Computing. Such a course, taught in the Stevens Institute of Technology, has been developed with much encouragement and help from Professor Daniel Duchamp (Director of Department of Computer Science), and many useful suggestions from Professor Dominic Duggan. Important insight, reflected in the course and in the book, came from graduate students who had served over the years as teaching assistants: Bo Ye (2012); Wa Gao (2013); Xiaofang Yu (2014); and Saurabh Bagde and Harshil Bhatt (2015).

It is owing to meeting (and subsequent discussions with) Professor Ruby Lee of Princeton University that we have learned of her research on *NoHype*—an alternative to traditional virtualization that addresses some essential security problems.

The past two years of working in the European Telecommunications Standardization Institute (ETSI) Network Function Virtualization (NFV) Industry Specification Group have contributed significantly to our understanding of the demands of the telecommunications industry. In particular, deep discussions of the direction of NFV with Don Clarke (Cable Labs), Diego Garcia Lopez (Telefonica), Uwe Michel (Deutsche Telekom) and Prodip Sen (formerly of Verizon and then HP) were invaluable in forming our perspective. Specifically on the subject of NFV security we owe much to all participants in the NFV Security group and particularly to Bob Briscoe (BT) and Bob Moskowitz (Verizon).

We got much insight into the US standards development on this topic in our conversation with George W. Arnold, then Director of Standards in National Institute of Standards and Technology (NIST).

It has been a great delight to work under the cheerful guidance of Ms Liz Wingett, our Project Editor at John Wiley & Sons. Her vigilant attention to every detail kept us on our feet, but the manuscript improved with every suggestion she made. As the manuscript was being prepared for production, Ms Audrey Koh, Production Editor at John Wiley & Sons, has achieved a feat truly worthy of the Fifth Labor of Hercules, going through the proofs and cleaning up the Augean Stables of stylistic (and, at times, even factual) inconsistencies.

To all these individuals we express our deepest gratitude.

CHAPTER 1
Introduction

> If the seventeenth and early eighteenth centuries are the age of clocks, and the later eighteenth and the nineteenth centuries constitute the age of steam engines, the present time is the age of communication and control.
>
> **Norbert Wiener** (from the 1948 edition of *Cybernetics: or Control and Communication in the Animal and the Machine*).

It is unfortunate that we don't remember the exact date of the extraordinary event that we are about to describe, except that it took place sometime in the Fall of 1994. Then Professor Noah Prywes of the University of Pennsylvania gave a memorable invited talk at Bell Labs, at which two authors[1] of this book were present. The main point of the talk was a proposal that AT&T (of which Bell Labs was a part at the time) should go into the business of providing computing services—in addition to telecommunications services—to other companies by actually running these companies' data centers. “All they need is just to plug in their terminals so that they receive IT services as a utility. They would pay anything to get rid of the headaches and costs of operating their own machines, upgrading software, and what not.”

Professor Prywes, whom we will meet more than once in this book, well known in Bell Labs as a software visionary and more than that—the founder and CEO of a successful software company, *Computer Command and Control*—was suggesting something that appeared too extravagant even to the researchers. The core business of AT&T at that time was telecommunications services. The major enterprise customers of AT&T were buying the *customer premises equipment* (such as private branch exchange switches and machines that ran software in support of call centers). In other words, the enterprise was buying things to run on premises rather than outsourcing things to the network provider!

Most attendees saw the merit of the idea, but could not immediately relate it to their day-to-day work, or—more importantly—to the company's stated business plan. Furthermore, at that very moment the Bell Labs computing environment was migrating from the Unix programming environment hosted on mainframes and Sun workstations to Microsoft Office-powered personal computers. It is not that we, who “grew up” with the Unix operating system, liked the change, but we were told that this was the way the industry was going (and it was!) as far as office information technology was concerned. But if so, then the enterprise would be going in exactly the *opposite* way—by placing computing in the hands of each employee. Professor Prywes did not deny the pace of acceptance of personal computing; his argument was that there was much more to enterprises than what was occurring inside their individual workstations—payroll databases, for example.

There was a lively discussion, which quickly turned to the detail. Professor Prywes cited the achievements in virtualization and massive parallel-processing technologies, which were sufficient to enable his vision. These arguments were compelling, but ultimately the core business of AT&T was networking, and networking was centered on telecommunications services.

Still, telecommunications services were provided by software, and even the telephone switches were but peripheral devices controlled by computers. It was in the 1990s that virtual telecommunications networking services such as *Software Defined Networks*—not to be confused with the namesake development in data networking, which we will cover in Chapter 4—were emerging on the purely software and data communications platform called *Intelligent Network*. It is on the basis of the latter that Professor Prywes thought the computing services could be offered. In summary, the idea was to combine data communications with centralized powerful computing centers, all under the central command and control of a major telecommunications company. All of us in the audience were intrigued.

The idea of computing as a public utility was not new. It had been outlined by Douglas F. Parkhill in his 1966 book [1].

In the end, however, none of us could sell the idea to senior management. The times the telecommunications industry was going through in 1994 could best be characterized as "interesting," and AT&T did not fare particularly well for a number of reasons.[2] Even though Bell Labs was at the forefront of the development of all relevant technologies, recommending those to businesses was a different matter—especially where a proposal for a radical change of business model was made, and especially in turbulent times.

In about a year, AT&T announced its trivestiture. The two authors had moved, along with a large part of Bell Labs, into the equipment manufacturing company which became Lucent Technologies and, 10 years later, merged with Alcatel to form Alcatel-Lucent.

At about the same time, Amazon launched a service called *Elastic Compute Cloud* (*EC2*), which delivered pretty much what Professor Prywes had described to us. Here an enterprise user—located anywhere in the world—could create, for a charge, *virtual* machines in the "Cloud" (or, to be more precise, in one of the Amazon data centers) and deploy any software on these machines. But not only that, the machines were *elastic*: as the user's demand for computing power grew, so did the machine power—magically increasing to meet the demand—along with the appropriate cost; when the demand dropped so did the computing power delivered, and also the cost. Hence, the enterprise did not need to invest in purchasing and maintaining computers, it paid only for the computing power it received and could get as much of it as necessary!

As a philosophical aside: one way to look at the computing development is through the prism of dialectics. As depicted in Figure 1.1(a), with mainframe-

based computing as the *thesis*, the industry had moved to personal-workstation-based computing—the *antithesis*. But the spiral development—fostered by advances in data networking, distributed processing, and software automation—brought forth the Cloud as the *synthesis*, where the convenience of seemingly central on-demand computing is combined with the autonomy of a user's computing environment. Another spiral (described in detail in Chapter 2) is depicted in Figure 1.1(b), which demonstrates how the *Public Cloud* has become the *antithesis* to the *thesis* of traditional IT data centers, inviting the outsourcing of the development (via "*Shadow IT*" and *Virtual Private Cloud*). The synthesis is *Private Cloud*, in which the Cloud has moved computing back to the enterprise but in a very novel form.

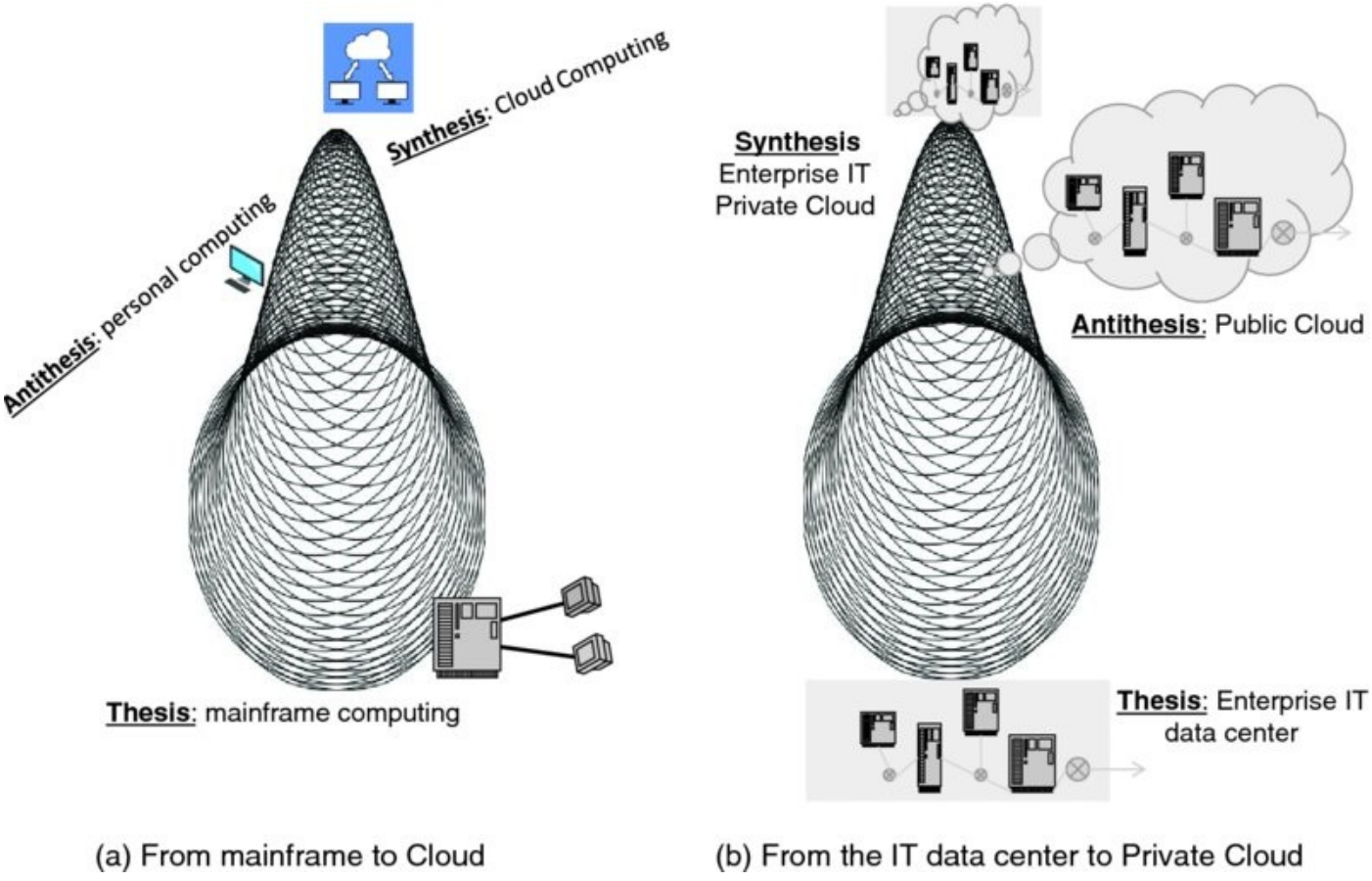

Figure 1.1 Dialectics in the development of Cloud Computing: (a) from mainframe to Cloud; (b) from IT data center to Private Cloud.

At this point we are ready to introduce formal definitions, which have been agreed on universally and thus form a standard in themselves. The definitions have been developed at the National Institute of Standards and Technology (NIST) and published in [2]. To begin with, Cloud Computing is defined as a model "for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." This Cloud model is composed of five essential characteristics, three service models, and four deployment models.

The five essential characteristics are presented in Figure 1.2.

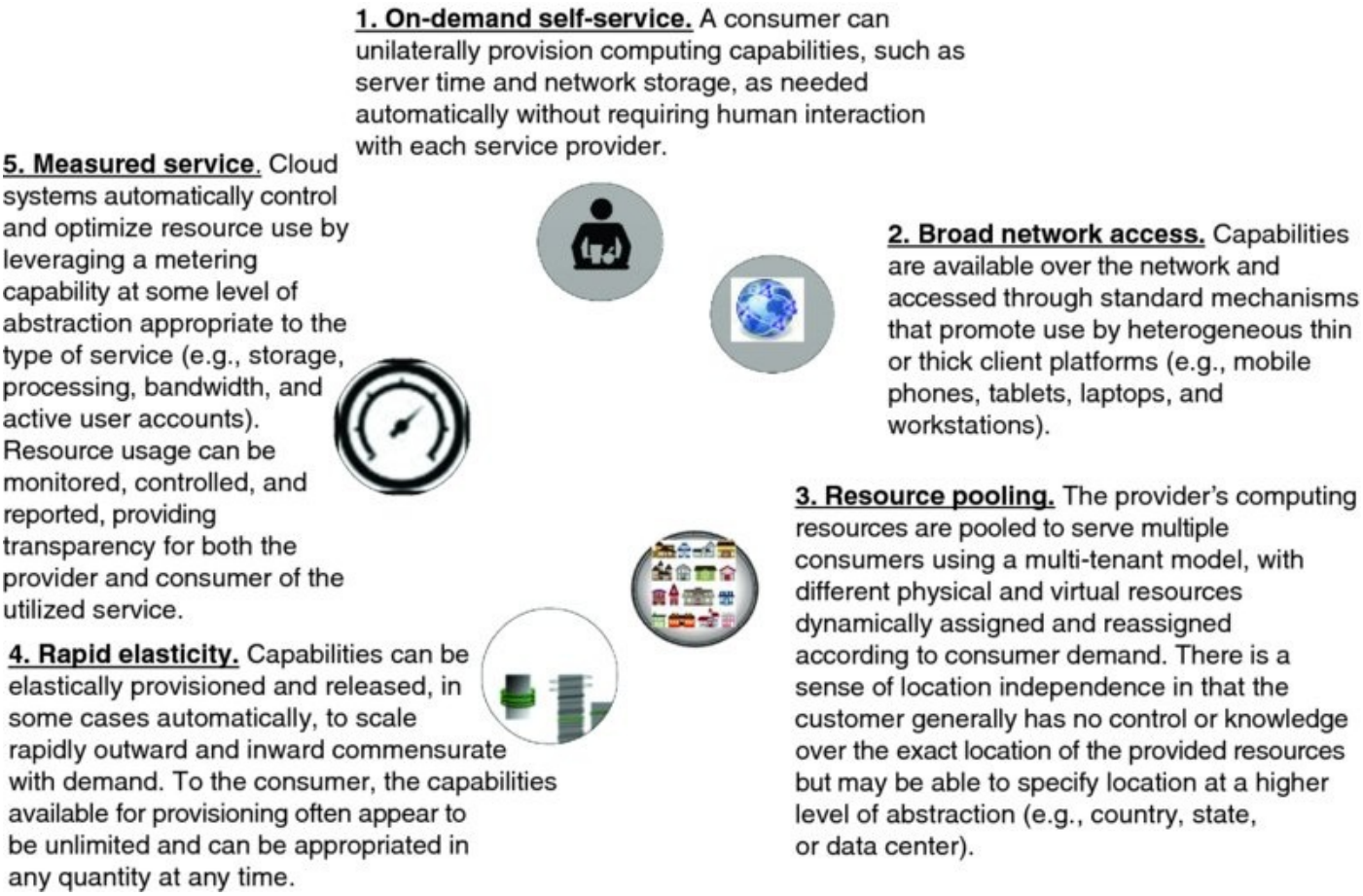

Figure 1.2 Essential characteristics of Cloud Computing. *Source:* NIST SP 800-145, p. 2.

The three service models, now well known, are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). NIST defines them thus:

1. *Software-as-a-Service* (*SaaS*). The capability provided to the consumer is to use the provider's applications running on a Cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based e-mail), or a program interface. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
2. *Platform-as-a-Service* (*PaaS*). The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

3. *Infrastructure-as-a-Service* (*IaaS*). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying Cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Over time, other service models have appeared—more often than not in the marketing literature—but the authors of the well-known "Berkeley view of Cloud Computing" [3] chose to "eschew terminology such as 'X as a service (XaaS),'" citing the difficulty of agreeing "even among ourselves what the precise differences among them might be," that is, among the services for some values of X...

Finally, the four Cloud deployment models are defined by NIST as follows:

1. *Private Cloud*. The Cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
2. *Community Cloud*. The Cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
3. *Public Cloud*. The Cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the Cloud provider.
4. *Hybrid Cloud*. The Cloud infrastructure is a composition of two or more distinct Cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., Cloud bursting for load balancing between Clouds).

Cloud Computing is not a single technology. It is better described as a business development, whose realization has been enabled by several disciplines: computer architecture, operating systems, data communications, and network and operations management. As we will see, the latter discipline has been around for as long as networking, but the introduction of Cloud Computing has naturally fueled its growth in a new direction, once again validating the quote from Norbert Wiener's book that we chose as the epigraph to this book.

As Chapter 2 demonstrates, Cloud Computing has had a revolutionary effect on the information technology industry, reverberating through the

telecommunications industry, which followed suit. Telecommunications providers demanded that vendors provide software only, rather than "the boxes." There have been several relevant standardization efforts in the industry, and—perhaps more important—there have been open-source software packages for building Cloud environments.

Naturally, standardization was preceded by a significant effort in research and development. In 2011, an author[3] of this book established the *CloudBand* product unit within Alcatel-Lucent, where, with the help of Bell Labs research, the telecommunications Cloud platform has been developed. It was in the context of *CloudBand* that we three authors met and the idea of this book was born.

We planned the book first of all as a textbook on Cloud Computing. Our experience in developing and teaching a graduate course on the subject at the Stevens Institute of Technology taught us that even the brightest and best-prepared students were missing sufficient knowledge in Central Processing Unit (CPU) virtualization (a subject that is rarely taught in the context of computer architecture or operating systems), as well as a number of specific points in data communications. Network and operations management has rarely been part of the modern computer science curriculum.

In fact, the same knowledge gap seems to be ubiquitous in the industry, where engineers are forced to specialize, and we hope that this book will help fill the gap by providing an overarching multi-disciplinary foundation.

The rest of the book is structured as follows:

- Chapter 2 is mainly about "what" rather than "how." It provides definitions, describes business considerations—with a special case study of *Network Function Virtualization*—and otherwise provides a bird's eye view of Cloud Computing. The "how" is the subject of the chapters that follow.
- Chapter 3 explains the tenets of CPU virtualization.
- Chapter 4 is dedicated to networking—the nervous system of the Cloud.
- Chapter 5 describes network appliances, the building blocks of Cloud data centers as well as private networks.
- Chapter 6 describes the overall structure of the modern data center, along with its components.
- Chapter 7 reviews operations and management in the Cloud and elucidates the concepts of orchestration and identity and access management, with the case study of *OpenStack*—a popular open-source Cloud project.
- The Appendix delves into the detail of selected topics discussed earlier.

The references (which also form a bibliography on the respective subjects) are placed separately in individual chapters.

Having presented an outline of the book, we should note that there are three

essential subjects that do not have a dedicated chapter. Instead, they are addressed in each chapter inasmuch as they concern that chapter's subject matter.

One such subject is security. Needless to say, this is the single most important matter that could make or break Cloud Computing. There are many aspects to security, and so we felt that we should address the aspects relevant to each chapter within the chapter itself.

Another subject that has no “central” coverage is standardization. Again, we introduce the relevant standards and open-source projects while discussing specific technical subjects. The third subject is history. It is well known in engineering that many existing technical solutions are not around because they are optimal, but because of their historical development. In teaching a discipline it is important to point these out, and we have tried our best to do so, again in the context of each technology that we address.

Notes

[1] Igor Faynberg and Hui-Lan Lu, then members of the technical staff at Bell Labs Area 41 (Architecture Area).

[2] For one thing, the regional Bell operating companies and other local exchange carriers started to compete with AT&T Communications in the services market, and so they loathed buying equipment from AT&T Network Systems—a manufacturing arm of AT&T.

[3] Dor Skuler, at the time Alcatel-Lucent Vice President and General Manager of the *CloudBand* product unit.