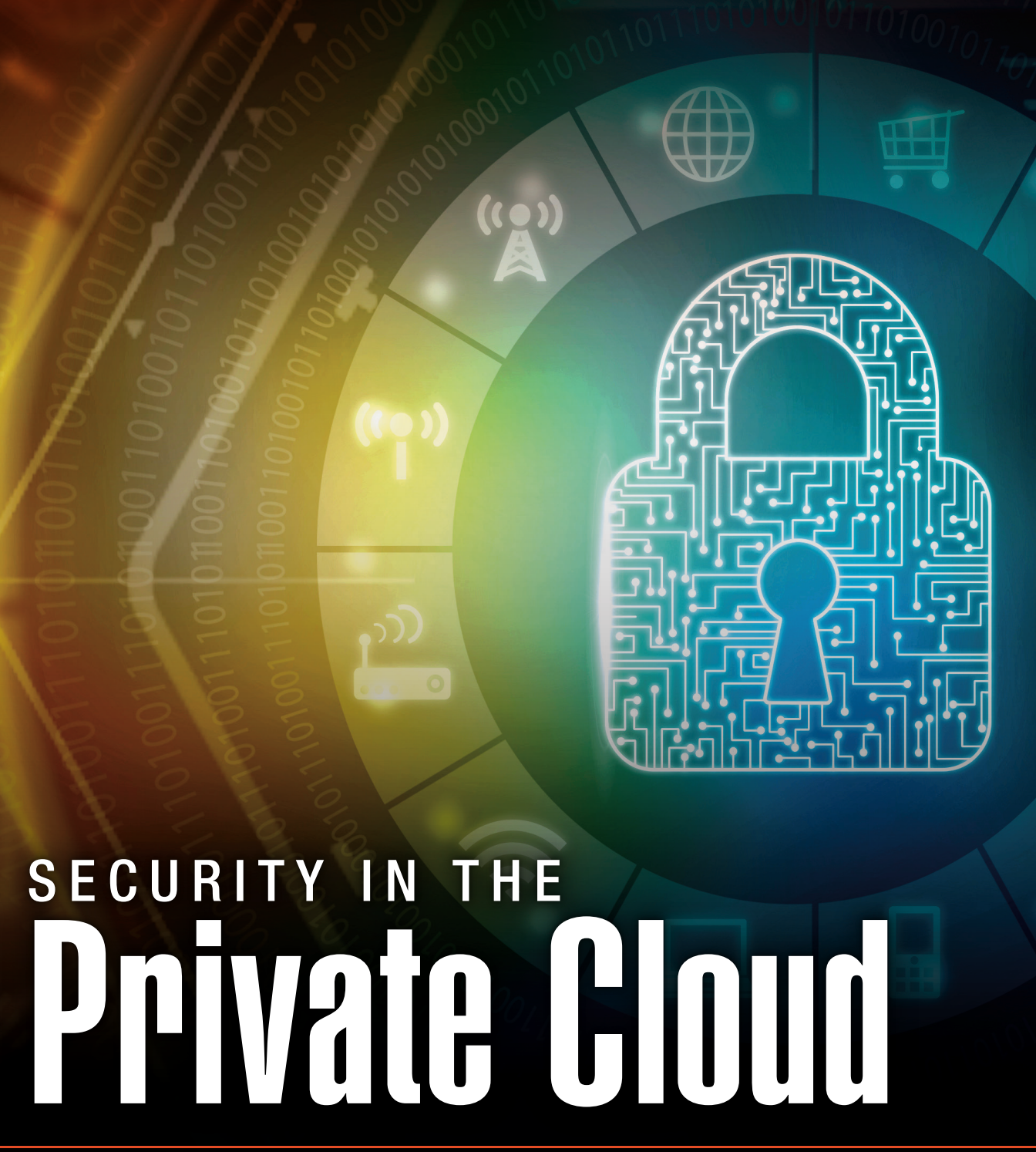

SECURITY IN THE Private Cloud

EDITED BY

JOHN R. VACCA

CRC Press
Taylor & Francis Group

SECURITY IN THE
Private Cloud

SECURITY IN THE

Private Cloud

EDITED BY

JOHN R. VACCA

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20160628

International Standard Book Number-13: 978-1-4822-5955-1 (Hardback)

Library of Congress Cataloging-in-Publication Data

Names: Vacca, John R., editor.
Title: Security in the private cloud / editor, John R. Vacca.
Description: Boca Raton : Taylor & Francis, a CRC title, part of the Taylor & Francis imprint, a member of the Taylor & Francis Group, the academic division of T&F Informa, plc, [2017] | Includes bibliographical references and index.
Identifiers: LCCN 2016024366 | ISBN 9781482259551 (hardback)
Subjects: LCSH: Cloud computing--Security measures. | Computer networks--Security measures.
Classification: LCC QA76.585 .S4435 2017 | DDC 004.67/82--dc23
LC record available at https://lccn.loc.gov/2016024366

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

This book is dedicated to my wife, Bee.

Contents

Foreword

Private clouds are very handy to have. An enterprise can load up its private cloud with a wide variety of applications and resources for users to access from almost anywhere. This makes things easier for the user and can simplify the requirements for building a complex network.

However, your private cloud will still require security as a computing environment as a whole, as well as for the individual applications and resources in the cloud. This requires layered security that first provides user access to the cloud, or parts of it, and then specific user rights for various applications. Resources may also need to be segregated in a manner that an unauthorized user may not even know the existence of some applications or data.

In this book, John R. Vacca provides the applicable knowledge and experience to help you secure your private cloud, the applications in your cloud, and the data stored in your cloud. Let's face it: we are in the age of hacks, cracks, and data theft. There are external threats as well as internal threats. You need to protect your cloud-based assets, and this book will help you do that.

Michael Erbschloe
Webster University

Michael Erbschloe teaches information security courses at Webster University in St. Louis, Missouri.

Preface

SCOPE OF COVERAGE

This comprehensive handbook serves as a professional reference as well as a practitioner's guide to today's most complete and concise view of private cloud security. The handbook defines private cloud computing security and establishes a strong working knowledge of the concepts and technologies needed to migrate your data center into a private cloud security solution. The knowledge you gain will enable you to determine whether the private cloud security solution is appropriate for your organization from a business and technical perspective to select the appropriate cloud security model and to plan and implement a cloud security adoption and migration strategy. Furthermore, this handbook will show you how to work with on- and off-premises private cloud computing security technologies and obtain practical experience in implementing security for private clouds. In the handbook, there is an emphasis on the layers of security associated with private cloud security implementations.

The primary audience for this handbook consists of engineers/scientists interested in monitoring and analyzing specific measurable private cloud computing security environments, which may include transportation and/or infrastructure systems, mechanical systems, seismic events, and underwater environments. This book will also be useful for security and related professionals interested in tactical surveillance and mobile private cloud computing security target classification and tracking; other individuals with an interest in using private cloud computing security to understand specific environments; undergraduate and graduate students; members from academia, government, and industry; anyone seeking to exploit the benefits of private cloud computing security technologies, including assessing the architectures, components, operation, and tools of private cloud computing; and anyone involved in the security aspects of private cloud computing who has knowledge at the level of the introduction to private cloud computing or equivalent experience. This comprehensive reference and practitioner's guide will also be of value to students taking upper division undergraduate- and graduate-level courses in private cloud computing security.

ORGANIZATION OF THIS BOOK

The book is organized into five sections composed of 20 contributed chapters by leading experts in their fields and three appendices, including an extensive glossary of cloud security terms and acronyms.

Section I: Introduction to Private Cloud Security

This section discusses private cloud computing essentials, which include cloud computing service models, namely, software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), and desktop as a service (DaaS); public, virtual private, and hybrid; and cyber security fundamentals. This section also covers private cloud security baselines and software and data segregation security.

Chapter 1, "Private Cloud Computing Essentials," sets the stage for the rest of the book, by presenting insight into how the cloud market is offering multiple options for businesses to transition their infrastructure, development platform, storage, and software. This chapter also covers how true innovation comes when successfully navigating the cloud space from traditional on-premise models to a recurring revenue model. Finally, it discusses how service providers are offering hybrid, private, and public cloud solutions, which lead to better efficiency, self-service, manipulation, and variety.

Chapter 2, "Integration of Enterprise Content Management and Software as a Service," explores the integration of enterprise content management systems with SaaS applications from the perspective of the user, that is, the enterprise. Terminology is defined, products are examined, security and risk considerations are raised, integration models are discussed, and examples of the integration between ECM systems and SaaS applications are provided.

Chapter 3, "Infrastructure as a Service," reviews the major components of a private cloud infrastructure to help you think about the security of that architecture. Next, it discusses a few high-level conceptual issues. Then, the chapter actually breaks down a cloud infrastructure into its various component pieces.

Chapter 4, "Preservation as a Service for Trust," addresses the difficulty in preserving digital information over the long term with its inherent risks of loss or corruption, and how the ITrust project is generating the theoretical and methodological frameworks necessary to develop local, national, and international policies; procedures; regulations; standards; and legislation that is able to ensure public trust in digital records. In support of this goal, the authors show how ITrust established the preservation as a service for trust (PaaST) project in order to develop a set of requirements that establish a foundation for trusting the preservation of digital information.

Chapter 5, "Software and Data Segregation Security," examines data segregation in cloud landscape, which is dictated through the allocation of a universal nonrepudiated subscribe identity. It also discusses the changes the conventional internal business system concept, because all cloud services subscribers are expected to share a single instance of computing power, database, network, cloud front end, and data resilience.

Section II: Achieving Security in a Private Cloud

This section discusses how to take full responsibility for cyber security by managing the risks of public clouds and identifying and assigning security tasks in each SPI service model: SaaS, PaaS, and IaaS. Next, it shows how to select the appropriate product, by comparing product-specific security features and organizational implementation requirements.

It focuses on the virtual private cloud (VPC) by showing how to simulate a private cloud in the public environment: Google Secure Data Connector and Amazon VPC. It also covers the hybrid cloud alternative by connecting on-premises data with cloud applications, securely bridging with VPC, and expanding capacity to meet business surges. Finally, it explains identification and privacy in the cloud.

Chapter 6, "Taking Full Responsibility for Cyber Security in the Private Cloud," discusses how cyber criminals create an unprecedented challenge to corporate information professionals on critical information asset protection. It also discusses why migration to cloud environments leads to diverse difficulty.

Chapter 7, "Selecting the Appropriate Product," explores the difference between the conventional internal enterprise information evaluation and how the cloud computing environment spans across the internal network and the Internet. It also explores the difference between the conventional internal enterprise information evaluation, how the cloud computing environment spans across the internal network, and the Internet; as well as, how it applies to the hybrid cloud environment. Finally, it focuses on how the selection of cloud computing services starts with a management initiative to take a risk-based approach.

Chapter 8, "Virtual Private Cloud," discusses that with the implementation of the VMware vCloud Suite, the foundation for IaaS will be built, and it is essential for delivering these use cases. It presents the core components of the vCloud Suite: vSphere and vCloud Director (VCD). Then, it specifies the design requirement for two vSphere clusters: an existing production cluster that will be used to host management components and a new two-node cluster that will serve as the initial resource cluster. In addition, it then focuses on the single VCD cell that will be deployed to provide access to the VCD environment. Finally, it shows that by leveraging a vCloud Suite, an IT department will be able to deliver IaaS functionality to the business and increase the overall performance, management efficiency, availability, and recoverability of the test, development, and training infrastructure.

Chapter 9, "Security in the Virtual Private Cloud," explains how VPC evolves naturally in the cloud computing landscape to address risks, vulnerabilities, and business concerns in public and community cloud. It also explains how private cloud attempts to address the security gaps in the emerging cloud computing architecture. Finally, it discusses how more development in VPC can be noted in the following areas: virtual partitioning, fine-grained privacy level, configurable security, and access controls.

Section III: Implementing Security in a Private Cloud

This section discusses the characteristics of private cloud security solutions, such as identifying public and private cloud security technologies and defining a generic public and private cloud security framework. Next, it explores how to transition security to a private cloud, which includes migrating a data center to the cloud by identifying critical performance metrics and autonomic computing with a private cloud. Then, it shows how to secure the management of virtualized resources. It also shows how to improve utilization with virtualization by choosing para- or hardware-assisted virtualization, utilize cores and hyperthreading, calculate the performance of EC2 Compute Units, and compare virtualization

and cloud computing. It then presents the deployment of an on-premises system center virtual machine manager (VMM) private cloud through a discussion of virtualizing with Microsoft Hyper-V hypervisor, which includes validating with Microsoft Assessment and Planning Toolkit, creating three types of virtual networks, and matching virtual CPUs to logical CPUs. Next, it covers aggregating virtual cloud resources with VMM (managing the cloud via the VMM Administrator Console, generalizing virtual machine templates and defining profiles, and provisioning users with role-based access control); creating images (performing Physical to virtual (P2V) and Virtual to Virtual (V2V) migrations and organizing VMM library resources); and deploying virtual machines (template-based, shared ISO images, and overwriting a virtual hard drive [VHD]). Then, it presents a description of how to monitor private cloud resources with a system center operations manager, which includes leveraging management packs (monitoring computers, devices, services, and applications, and creating a resource pool) and reporting on the private cloud operation (audit collection services reporting and tracking service levels). Next, it covers continuous private cloud monitoring and shows how to manage a private cloud with a system center service manager, such as leveraging the cloud services process pack (creating a cloud-based pricing chargeback process, automating the deployment of tested Integration as a Service [IASS], and requesting cloud resources with self-service), automating the private cloud (deploying service request catalogs and fulfilling service requests with an orchestrator), and adapting your IT service best practices (incident and problem resolution, change control, asset life cycle management, Microsoft Operations Framework, and Information Technology Infrastructure Library). Next, it shows how to deploy a hosted Amazon VPC, which includes evaluating the benefits of a VPC (creating multiple private and public networks, controlling packets with network access control lists (ACLs), and routing and leveraging elastic network interfaces), and how to deploy a VPC and launch instances (selecting from preset VPC configurations and applying a Classless Inter-Domain Routing address). Then, it describes how to secure a private cloud, such as identifying security weak spots (assessing vulnerabilities and hacking private clouds, and evaluating Amazon Machine Image security) and meeting governance requirements (securing with IT GRC Process Management Pack and protecting users with the Data Protection Manager). This section then discusses cloud security assessment and authorization. It shows a presentation of how to create a hybrid cloud solution, which includes expanding your private cloud (handling excess demand with cloud bursting, connecting your cloud with a virtual private network, and monitoring hybrid cloud with AWS Management Pack) and evolving to hybrid clouds (exploiting the advantages of hybrid clouds and examining hybrid cloud use cases). Finally, it presents an analysis of joint security and privacy aware protocol design.

Chapter 10, "The Hybrid Cloud Alternative," discusses how the hybrid cloud is a promising option to address practical business concerns. It also explains how the current public and private cloud solutions can only handle isolated business situations. It then describes how continuous merger and acquisition complicate business landscape to demand a quick provision and deployment approach. It focuses on why hybrid cloud is a blending of all known cloud technologies. Finally, it explains why OpenStack is an open source to realize this paradigm of hybrid cloud.

Chapter 11, "Identification and Privacy in the Secure Cloud," discusses the concept of identity authentication and its implication for cloud systems. It also discusses the fundamentals of identity in the cloud, the concept of identity assurance, and the considerations for selection of identity authentication technologies and models for the cloud.

Chapter 12, "Private Cloud Security and Identification," examines various identity management and encryption approaches, in order to elaborate the value contribution to the general cloud ecosystem.

Chapter 13, "Secure Management of Virtualized Resources," introduces security issues and solutions. It further delves into virtual resource management. In particular, it deals with real hardware offering virtual resource sharing to cloud hosts, tasks, and services. In order to do that, it further describes the characteristics of the current technology.

Chapter 14, "Designing Cloud Security and Operations Models in the Changed Geopolitical Environment," outlines some of the challenges and developments in the world that could make the usage of cloud more complicated because of newly emerging country specific laws, regulations, and industry standards.

Chapter 15, "Continuous Private Cloud Security Monitoring," outlines some core principles and best practices for security monitoring of IT systems, especially within the context of cloud, and points out the cloud-specific activities that must be considered by a cloud system administrator.

Chapter 16, "Cloud Security Assessment and Authorization," reviews assessment and authorization methods, and activities for cloud-based information systems.

Chapter 17, "Assessment and Authorization in Private Cloud Security," discusses various cloud computing security issues, in particular, those regarding authorization and security assessment. It introduces security challenges and approaches, which result in a broad survey that tries to shed a light on security issues of cloud computing, mainly focusing on the issues related to security assessment and authorization. Based on the survey, this chapter discusses the differences between the various approaches; some are still evolving, and their security has yet to be improved further, whereas others are more technically mature.

Section IV: Advanced Private Cloud Computing Security

This section focuses on advanced private cloud computing security, advanced failure detection and prediction, future directions in private cloud computing security risks and challenges, private cloud computing with advanced security services, and advanced security architectures for private cloud computing.

Chapter 18, "Advanced Security Architectures for Private Cloud Computing," addresses the scope and the nature of privacy and security within the private cloud computing infrastructure.

Chapter 19, "Advanced Private Cloud Computing Security Architectures," shows how security is a process and a mind-set. It also discusses how deploying a private cloud is clearly quite different than on-ramping services to a public cloud. Then, it shows how analyzing every situation from many different angles is the nature of most security professionals, and, when architecting security, a private cloud environment of this quality will be put to the test. Finally, it describes how maintaining a high level of security maturity

by performing due diligence and producing strong policies around all your processes will help you lead a successful, robust, and secure private cloud implementation.

Chapter 20, "Privacy Protection in Cloud Computing through Architectural Design," introduces architectural designs for privacy protections in clouds. In this chapter, the authors describe their basic assumptions about the cloud computing environment and discuss what kind of threats are considered in architectural designs. Next, they assume that the swapped pages are encrypted in order to protect the guest VM space. Finally, they describe the privacy protection problem in cloud computing.

John R. Vacca
TechWrite

Acknowledgments

There are many people whose efforts on this book have contributed to its successful completion. I owe each a debt of gratitude and offer my sincere thanks.

I express my very special thanks to my executive editor, Rick Adams, without whose continued interest and support this book would not have been possible, and to my editorial assistant, Sherry Thomas, who provided staunch support and encouragement when it was most needed. I thank my production editor, Cynthia Klivecka; project coordinator, Marsha Pronin; and copyeditor, Indumathi, S., whose fine editorial work has been invaluable. I also thank my marketing manager, Joanna Knight, whose efforts on this book have been greatly appreciated. Finally, I thank all of the other people at CRC Press (Taylor & Francis Group), whose many talents and skills are essential to a finished book.

I thank my wife, Bee Vacca, for her love, help, and understanding of my long work hours. Also, I express my very very special thanks to Michael Erbschloe for writing the foreword. Finally, I thank all the following authors who contributed chapters that were necessary for the completion of this book: Lauren Collins, Patricia C. Franks, Mario Santana, Luciana Duranti, Adam Jansen, Giovanni Michetti, Courtney Mumma, Daryll Prescott, Corinne Rogers, Kenneth Thibodeau, Daniel Ching Wa, Sarbari Gupta, Roberto Di Pietro, Flavio Lombardi, Matteo Signorini, Thorsten Herre, Pramod Pandya, Riad Rahmo, Albert Caballero, Wanyu Zang, Meng Yu, and Peng Liu.

Editor

John R. Vacca is an information technology consultant, professional writer, editor, reviewer, and internationally known, best-selling author based in Pomeroy, Ohio. Since 1982, Vacca has authored/edited 77 books; some of his most recent books include the following:

- *Handbook of Sensor Networking: Advanced Technologies and Applications* [Publisher*:* CRC Press (an imprint of Taylor & Francis Group, LLC) (January 14, 2015)]
- *Network and System Security,* second edition [Publisher*:* Syngress (an imprint of Elsevier, Inc.) (September 23, 2013)]
- *Cyber Security and IT Infrastructure Protection* [Publisher*:* Syngress (an imprint of Elsevier, Inc.) (September 23, 2013)]
- *Managing Information Security,* second edition [Publisher*:* Syngress (an imprint of Elsevier, Inc.) (September 23, 2013)]
- *Computer and Information Security Handbook,* second edition [Publisher*:* Morgan Kaufmann (an imprint of Elsevier, Inc.) (May 31, 2013)]
- *Identity Theft (Cybersafety)* [Publisher*:* Chelsea House Pub (April 1, 2012)]
- *System Forensics, Investigation, and Response* [Publisher*:* Jones & Bartlett Learning (September 24, 2010)]
- *Managing Information Security* [Publisher*:* Syngress (an imprint of Elsevier, Inc.) (March 29, 2010)]
- *Network and Systems Security* [Publisher*:* Syngress (an imprint of Elsevier, Inc.) (March 29, 2010)]
- *Computer and Information Security Handbook, 1E* [Publisher*:* Morgan Kaufmann (an imprint of Elsevier, Inc.) (June 2, 2009)]
- *Biometric Technologies and Verification Systems* [Publisher*:* Elsevier Science & Technology Books (March 16, 2007)]
- *Practical Internet Security* (Hardcover) [Publisher*:* Springer (October 18, 2006)]

- *Optical Networking Best Practices Handbook* (Hardcover) [Publisher: Wiley-Interscience (November 28, 2006)]
- *Guide to Wireless Network Security* [Publisher: Springer (August 19, 2006)]
- *Computer Forensics: Computer Crime Scene Investigation* (with CD-ROM), 2nd Edition [Publisher: Charles River Media (May 26, 2005)]

He has published more than 600 articles in the areas of advanced storage, computer security, and aerospace technology (copies of articles and books are available upon request). He was also a configuration management specialist, computer specialist, and the computer security official for the National Aeronautics and Space Administration (NASA)'s space station program (Freedom) and the International Space Station Program, from 1988 until his retirement from the NASA in 1995.

In addition, Vacca is also an independent online book reviewer and was one of the security consultants for the MGM movie titled *AntiTrust*, which was released on January 12, 2001. A detailed copy of his biography can be viewed at http://www.johnvacca.com. He can be reached at john2164@windstream.net.

Contributors

Albert Caballero
HBO Latin America Group
Caracas, Venezuela

Daniel Ching Wa
Kun Hang Group
and
HK University of Science and Technology
and
HK Polytechnic University
and
University of Hong Kong
Hong Kong, China

and

Jiangxi University of Finance and Economics
Nanchang, China

Lauren Collins
Winning Edge Communications
New Lennox, Illinois

Roberto Di Pietro
Alcatel Lucent Bell Labs
Boulogne-Billancourt, France

Luciana Duranti
Archival Studies
School of Library, Archival and Information Studies
The Irving K. Barber Learning Centre
University of British Columbia
Vancouver, British Columbia, Canada

Patricia C. Franks
School of Information
San Jose State University
San Jose, California

Sarbari Gupta
Electrosoft Services, Inc.
Reston, Virginia

Thorsten Herre
Security and Compliance Office
Cloud and Infrastructure Delivery
SAP SE
Walldorf, Germany

Adam Jansen
School of Library, Archival and Information Studies
University of British Columbia
Vancouver, British Columbia, Canada

Peng Liu
Pennsylvania State University
University Park, Pennsylvania

Flavio Lombardi
Istituto per le Applicazioni del Calcolo, IAC-CNR
Rome, Italy

Giovanni Michetti
Department of Document Studies, Linguistics and Geography
Sapienza University of Rome
Rome, Italy

Courtney Mumma
The Internet Archive
San Francisco, California

Pramod Pandya
Department of Information Systems and Decision Sciences
Mihaylo College of Business and Economics
California State University
Fullerton, California

Daryll Prescott
Independent Consultant
Government Domain Task Force
Dickinson, North Dakota

Riad Rahmo
Independent Researcher and Consultant
California State University, Fullerton
Mission Viejo, California

Corinne Rogers
School of Library, Archival and Information Studies
University of British Columbia
Vancouver, British Columbia, Canada

Mario Santana
Terremark Worldwide, Inc.
Miami, Florida

Matteo Signorini
Pompeu Fabra University
Barcelona, Spain

Kenneth Thibodeau
Independent Researcher
Centre for the International Study of Contemporary Records and Archives
Evergreen, Colorado

Meng Yu
University of Texas at San Antonio
San Antonio, Texas

Wanyu Zang
Texas A&M at San Antonio
San Antonio, Texas

I

Introduction to Private Cloud Security

CHAPTER 1

Private Cloud Computing Essentials

Lauren Collins

CONTENTS

1.1 INTRODUCTION

Cloud computing is a service model delivering on-demand computing resources over the Internet. This cloud model is composed of five essential characteristics, three service models, and four deployment models [1]. Cloud computing features all aspects of modern-day technology and affects the users, process, and technology of an enterprise; cloud infrastructures are scalable, readily available, accessible, and elastic. There are several tools at our disposal for consuming data across thousands of machines. Businesses are able to run an entire development environment, even an entire company, without procuring or housing a physical enterprise grid of hardware and resources. Today, virtually all businesses are using cloud services and may not even be aware of it. There are countless benefits derived

from cloud infrastructures addressing business needs and delivering simplicity in order to accelerate growth and innovation.

Although there are numerous characteristics defining cloud computing, the following list summarizes the scope of cloud data, applications, services, and infrastructure:

- *Hosting*: platform, services, or data accessed are hosted on remote infrastructure.
- *Ubiquitous*: platform, services, or data are accessible from any location at anytime.
- *Commodity*: pay by use, customizable, and scalable.

Cloud computing characteristics can be further divided into two groups: essential characteristics and common characteristics, as shown in Figure 1.1.

The National Institute of Standards and Technology (NIST) lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. It also lists three "service models" (software, platform, and infrastructure) and four "deployment models" (private, community, public, and hybrid) that together categorize ways to deliver cloud services. The definition is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing [2]. A consumer is able to unilaterally provision computing capabilities, referred to as on-demand self-service, and is customarily done through a web-based portal or management console. Server up-time and allocation of network storage can be predefined and increased automatically without the need for human interaction from each service provider ("service provider refers to departments of information technology [IT]: server team, storage team, etc."). Broad network access provides competencies available over the network, accessed through typical mechanisms, which promote use by assorted client platforms (laptop, mobile devices, etc.). Resource pooling refers to the independence and availability of resources, such as processing power, memory allocation, storage, network bandwidth, and virtual machines (VMs). Usually, a

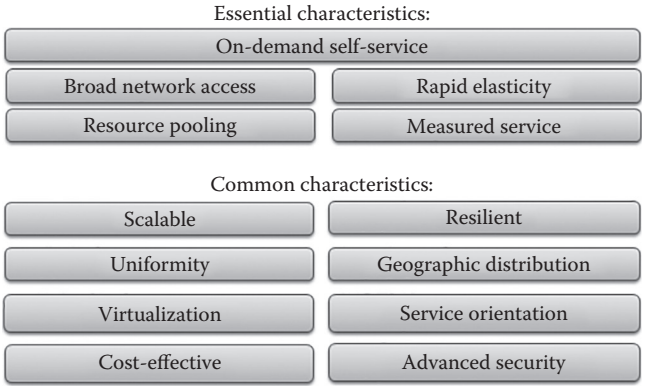

FIGURE 1.1 Cloud computing composed of five essential characteristics and eight common characteristics.

consumer is unaware (and has no control) of the exact location of resources provided to their platform. Resource pooling effectively establishes the concept for presenting and consuming resources in a consistent and transparent manner. Subsequently, capabilities can be rapidly and elastically provisioned instantaneously and automatically. To the consumer, the capabilities available for provisioning resources appear to be limitless and therefore can be purchased and allocated in any quantity at any time. With that being said, cloud platforms regulate and augment resources by gauging some level of abstraction appropriate to the service type (e.g., processing, memory, bandwidth, storage) by user group and account. Service providers such as Amazon, Google, Microsoft, and Rackspace provide numerous infrastructures spatially located in segregate grids, allowing for robust capacity and minimal downtime. Their cloud solutions entertain mirrored solutions, offering a resilience that gives businesses the necessary sustainability during unforeseen events. Regardless of the chosen provider, the cloud model makes it easy for businesses to work with clients, even if they use an entirely different service provider. Further elaboration of the five essential features of cloud computing is as follows:

1. *On-demand self-service*: IT provisions VMs for their internal customers, departments. Users have the ability to provision cloud computing resources using either a web portal or management console, all without human interaction.
2. *Broad network access*: Connectivity is only for internal customers, departments, accomplished by either local network access or connection to a virtual private network (VPN). Many client platforms are supported, such as the use of mobile devices, laptops, and workstations.
3. *Resource pooling*: Multiple customers are able to use the same physical resources, by segregating logical resources in a secure environment.
4. *Rapid elasticity*: IT provisions VMs by selecting the operating system (OS) and software, but now resources can be provisioned and released based on predefined parameters. Environments do not outgrow themselves too quickly and starve for resources, and an application will have the amount of necessary capacity at any point in time.
5. *Measured service*: The use of resources is monitored and then reported, or billed transparently back to a business unit based on utilization. Chargeback is accomplished by allocating budgets by department, rather than measuring actual usage.

Separately, these platforms conceal the complexity and level of specificity of the underlying infrastructure from the user and their applications by providing an easy-to-use graphical interface or applications programming interface. In addition, such a platform provides on-demand services that are always accessible from anywhere at anytime. Cloud service offerings have irrevocably changed the way software is deployed. Yet, the majority of organizations are slow to adopt cloud-based architectures; therefore, security concerns steer enterprises toward a private cloud deployment. Services are accessed via an interface that requires thorough design from an architect.

1.2 CLOUD COMPUTING SERVICE MODELS

In effort to appreciate the business value of cloud computing, it is essential to first identify the components, and then determine the capacity in which it can be utilized. Cloud computing describes such a broad range of services but is ultimately a model for facilitating accessible, on-demand access to a shared pool of resources that can quickly be provisioned with minimal user or administration interaction. The three service models of cloud computing are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Table 1.1 illustrates the comparison of service and sourcing models of cloud computing.

The core concepts and configurations of cloud computing are used throughout most service providers and implementations. Robust architecture is of the utmost importance in which service delivery is referenced; the methodology, sourcing, and regulation of a cloud computing environment will extend an available, scalable, and agile solution. IT must adjust their logic from individual, specific deployment models to delivering a predetermined and standard deployment. This strategy will become the norm as more organizations choose the cloud to meet their specific needs.

1.2.1 Infrastructure as a Service

IaaS incorporates vendor-managed network appliances, storage, servers, and virtualization layers in which consumers run their application and store data. Countless benefits are present when using IaaS, but every service provider offers a little different platform. Most have heard of Amazon's offering of cloud services; QualiSystems' CloudShell is unique in which they are based on the model of mixed infrastructure environments that can support any variety of infrastructures connected in any manner. For instance, CloudShell is able to support both on-premise and public cloud servers along with mainframe sessions

TABLE 1.1 The Cloud Computing Model Incorporating IaaS, PaaS, and SaaS

Type	Consumer	Service Provided	Service-Level Coverage	Customization
IaaS	• Application owner of IT provides OS • Application and middleware support	• Virtual server • Cloud storage	• Virtual server availability • Provisioning time • No platform or application coverage	• Minimal constraints on application installed on standardized virtual OS builds
PaaS	• Application owner	• Runtime environment for application • Cloud storage • Additional cloud services such as integration	• Environment availability • Environment performance • No application coverage	• Robust application level of customization available within constraints of services offered
SaaS	• End user	• Finished application	• Application uptime • Application performance	• Minimal to no customization • Capabilities dictated by market or service provider

connected along with legacy Unix servers. Various networking topologies are also supported; whether using virtual switches, software-defined networking switches, or conventional layer 2 switches, seamless connectivity is present.

Consider the infrastructure requirements of a proprietary trading firm: the headquarter, and 35 of the desk traders, is located in Chicago, Illinois. A second, smaller office is located in Manhattan, New York, with only four desk traders. The traders from both offices actively trade on Singapore, Dubai, London, New York, and Chicago markets. Prior to cloud computing, the game of speed was played in which the pricing and order matching servers needed to be collocated in proximity to the respective markets. Figure 1.2 illustrates a network diagram relative to the infrastructure requirements described above.

Each market location requires collocated servers and a dedicated circuit for connectivity. The costs involved in this infrastructure are extraordinary; a dark fiber circuit, providing low-latency, high-frequency speed, could cost US$10,000, on average. Then, consider the cost of the actual space leased from the collocation along with the cost of physical servers and networking hardware, such as firewalls and switch gear. Figure 1.3 shows the required infrastructure in a typical collocation cabinet. Located at the top of the rack are network switches, establishing both site-to-site connectivity for each trading firm office location and cross-connects to respective market infrastructures, possibly located in the same room or another floor in the same building. Local server connections pictured in this figure also tie into the switches within the cabinet. The average cost for hardware pictured in this diagram is about US$200,000. Add in the time to design, configure, ship, and install this infrastructure and the total cost could near half a million dollars.

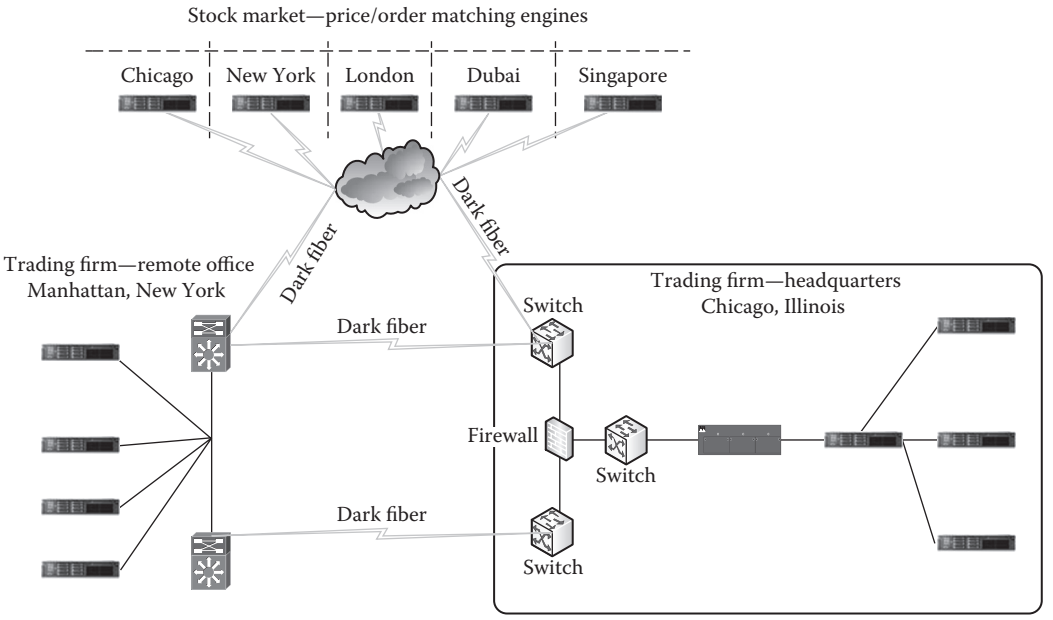

FIGURE 1.2 Infrastructure requirements prior to cloud computing architectures for a proprietary trading firm.

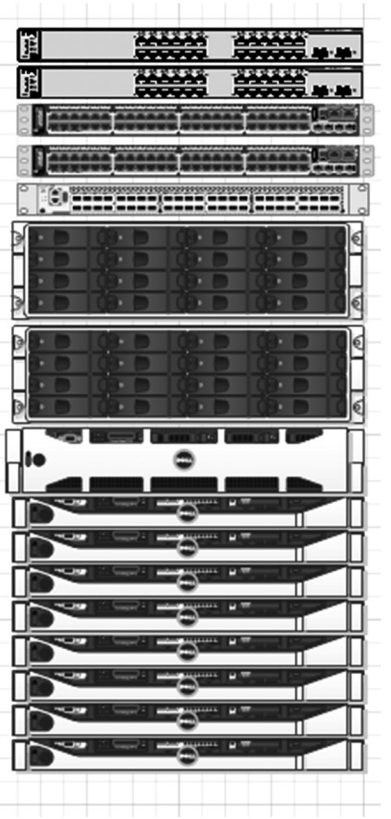

FIGURE 1.3 Typical collocated infrastructure for connectivity at one proprietary trading site.

The saying "time is money" resonates with IT management when deciding to move to a cloud infrastructure. The days of configuring equipment and shipping it all over the world are over. Not only does the amount of time for deployment decrease considerably, but resources can be allocated to other service areas as needs change or grow. And if a particular product is not traded any longer, the server does not sit in the cabinet collecting dust, using electricity, and cooling. Infrastructure engineers are able to focus on innovation and agility, and organizations can reallocate a substantial percentage of their budget on providing real value to clients rather than simply keeping the lights on. In an IaaS environment, the resources can be allocated to another deployment or can be turned off, saving money in a usage-based or pay-as-you-go program, which is discussed later in this chapter.

Now, consider the above physical requirements of hardware deployed into a pool of computing, storage, and network connectivity options delivered as a service. The consumer, or user, takes responsibility for the configuration of the OS and the necessary software and database. The goal is to create and provide a standard, flexible, virtualized environment that will become the foundation for PaaS and SaaS. IaaS has transformed organizations from being decidedly logistic driven to being vastly cloud driven, and businesses are appreciating pronounced payoffs from the transformation. Automation and self-service are the buzz words associated with cloud computing. When an infrastructure is carefully

architected and orchestrated, customers and business are able to operate in an agile manner, gaining efficiency and productivity. The industry moving toward cloud computing incorporates IaaS with its current, legacy infrastructure. Most IT and development teams are conflicted with their on-premise mixture of legacy and virtual hardware and applications infrastructure. An IaaS environment mitigates the risk of legacy application and server migrations, and sets the stage for effective cross-team collaboration, testing, and seamless integration and provisioning of products and services.

1.2.2 Platform as a Service

PaaS builds on top of IaaS, utilizing vendor-managed middleware applications, databases, and most commonly web portal software. It offers an agile approach to run scalable applications in a predictable, cost-effective fashion. Service levels and operational risks are now shared because the user accepts the responsibility for the configuration and operation of the application, and the provider delivers the platform resources (operational functionality and infrastructure). Figure 1.4 compares the process of delivering an application. On the legacy platform, once an application is requested by a development team, IT has to procure and build the server OS, install updates and service packs, then install relative software for developers to use the server, along with a bunch of other minor access details such as setting up user accounts and adding security groups. A cloud computing environment delivers an application in the matter of time it takes to open a browser. Furthermore,

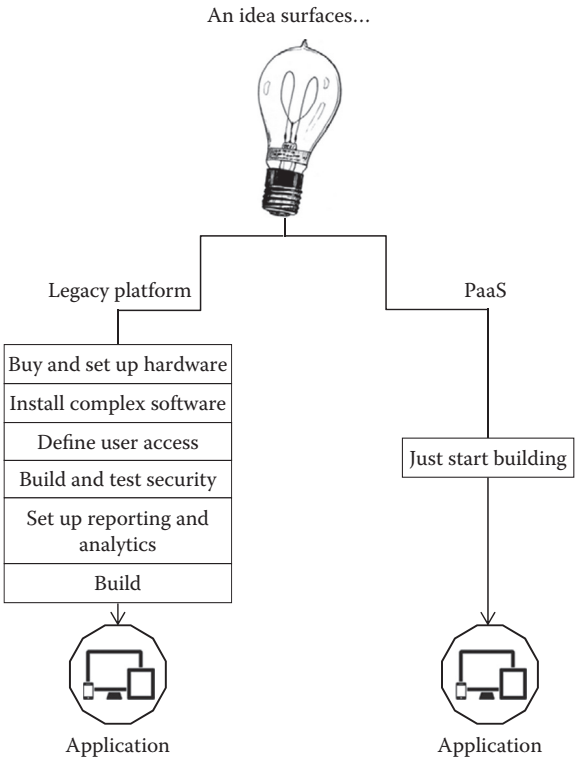

FIGURE 1.4 Compare the time to deliver an application using both a legacy platform (left) to PaaS.

PaaS applications have the latest features excluding the pain of constant upgrades and troubleshooting of those updates.

The legacy model of building and running on-premise applications is too complex, expensive, and slow. One application needs a lot of hardware, an OS, a database, and web servers, and may even require additional software. An entire application, network, systems, and server team were needed to keep everything running smoothly. Once a change or upgrade to the application was requested, another cycle of lengthy development, planning, testing, and deployment results; these cycles are a part of everyday business across all organizations. Aside from the painful, lengthy process to deploy an environment, applications built on this complex framework do not scale for usage demands nor business changes.

1.2.3 Software as a Service

SaaS provides substantial efficiencies in which cost and time to deployment are concerned, just as IaaS and PaaS. It is an innovative approach to distributing software, in which instead of selling to clients or businesses it is made available over the Internet using cloud computing methodology. Subsequently, providers host the software remotely, saving the additional investment in hardware and then charging the users with respect to the time spent using it or by paying a monthly fee. Access to applications is simplified, and no installation, deployment, or maintenance costs are incurred. Similar to IaaS and PaaS, a shift in operational risk is now on the provider rather than the client in a SaaS environment.

SaaS employs applications such as customer relationship management (CRM) (e.g., SalesForce), social performance management tools (e.g., SuccessFactors), tracking and monitoring solutions (e.g., Google Analytics), Professional Services Automation (e.g., Riverbed), and cloud integration applications. Figure 1.5 illustrates a SaaS deployment in which software is delivered as a service, primarily over a uniform resource locator.

1.2.4 Other Cloud Service Models

Organizations have expanded their horizons of cloud service offerings to further simplify the deployment of desktops, servers, storage, and even entire environments. Centralized management and rapid deployment save time and money when considering

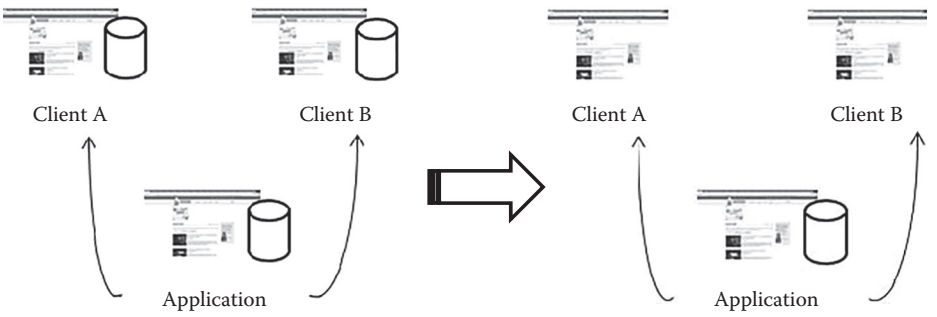

FIGURE 1.5 SaaS employing applications relevant to the user, such as e-mail, social analytics, document management, or CRM. The application database remains in the same location as the application (right) in a SaaS environment.

the management of devices as well as the physical footprint. The additional cloud services are as follows:

- Desktop as a service
- Hardware as a service
- Disaster recovery as a service
- Business process as a service
- Big data as a service

Data analytics and business intelligence have become an integral piece of organizations; therefore, consulting firms have added a fourth service model, business process as a service (BPaaS). Just as the other service models, BPaaS builds on top of all the other cloud service models and considers an entire spectrum of vertical or horizontal business process. In addition to all the service models, big data as a service is on the horizon.

1.3 PUBLIC CLOUD

The public cloud is defined as a multitenant environment, where a service provider makes resources, such as applications and storage, available to multiple users, known as the general public, over the Internet. Services available in the public cloud are usually free or use a pay-as-you-go model. Cloud service providers in this arena are Amazon Web Services, Google, SalesForce, and so forth. One use case of an organization's choice for a public cloud environment is when they desire to implement global or large-scale solutions, which would typically be out of reach without utilizing the cloud due to incurring significant costs or their IT staff lacks the expertise. Public cloud services deliver flexible, cost-effective implementations and facilitate access to cutting-edge technologies.

1.4 VIRTUAL PRIVATE CLOUD DESIGN

Generally, when discussing a "private cloud" environment, some are under the assumption that privacy and security are accomplished only by deploying physical hardware in private data center space. There are also some who believe cloud deployments only consist of virtualizing servers, implementation of management tools for provisioning of virtualization, and all connectivity and management happens on the local network. Those who make either or both assumptions will be enlightened to learn that you are on the right track; but, there is more. Virtualization can be a core component of cloud deployments, whether public or private.

1.4.1 Case 1: Virtualization

IT departments seem to be chasing their tails and finding the need for more resources as soon as they finish a deployment. They implement a virtualization solution, so they can quickly provision an infrastructure and consolidate servers. Not only are they able to provision storage space based on departmental needs, but they can also configure machines

with the hypervisor of choice and ample processing power and memory using management tools. Image files are created and uploaded to the management software, so a new OS can be installed on a VM. The environment must be connected to its local network for machine and resource management. Table 1.2 illustrates a key theory of cloud architecture, resource pooling, and abstraction of virtualized resources from an underlying virtual infrastructure. A number of constructs allocate capacity and resources by department, and are then charged back to internal department or client budgets, or the cost can be split between groups or locations, or simply track the number of machines deployed for each department.

1.4.2 Case 2: Private Cloud

A global software company's headquarters in Manhattan, New York, employ a central IT department that supports proprietary company-wide and department-specific applications. There are several additional locations each with a handful of local IT staff that focus on level 1 and 2 support of desktops or network tasks. Occasionally, a site may place an order for a server, then set it up on the domain itself, including all service packs, software, and network configuration. However, process could be streamlined by IT staff located

TABLE 1.2 A Number of Principles for Cloud Architecture Map to Virtual Data Centers for Resources

Virtualization Concept	Description
Provider virtual data center	Logical grouping of computing resources (attached virtual cluster of or more datastores) to provide cloud resources to consumers
Organization	Unit of administration that represents a logical collection of users, groups, and computing resources. Also serves as a security boundary from which only users of a particular organization can deploy workloads and have visibility into such workloads in the cloud. An organization is an association of related end users
Organization virtual data center	Subset allocation of provider virtual data center resources assigned to an organization, automatically backed by resource pool • Allocation • Reservation • Pay as you go
External network	Network that connects to the outside using an existing virtual network port group
Organization network	Network visible within an organization. External organization has connectivity to an external network using a direct or routed connection, or an internal network visible to apps within the organization
Network pool	Set of preallocated networks that can be allocated as needed to create private networks and network address translation (NAT)-routed networks
Virtual application	Preconfigured container of one or more VMs and virtual application networks
Virtual application network	Network visible within a virtual application, connected to other virtual application networks within an organization using a direct or routed connection, or internal network visible only to VMs within the virtual application
Virtual application templates and catalogs	Collection of available services for consumption. Catalogs contain virtual application template (preconfigured containers of one or more VMs) and/or media (images of operating systems)

in Manhattan procuring and implementing servers or applications. Given that not only can they provide better centralized support for remote branches, but they also have the ability to deliver servers with predefined, benchmark-tested specifications, and deploy storage in their preferred manner. IT headquarters also possess the image file for server or VMs, complete with preinstalled and configured OS and drivers. Furthermore, management software permits various users of distinctive access levels to perform tasks such as launching VMs, installing VMs from images, rebooting machines or tweaking memory or processing specifications, and configuring virtual networks between VMs.

Instantaneously, the remote sales department is able to login to a portal, spin up a new VM with the latest release of their proprietary software, and use it for a few days for testing. If something breaks or has to be redone, the VM can be turned off, reconfigured, or deleted without impacting the production version of the current software. Engineering and development teams will usually deploy several VMs to test the new software and act as a staging environment, having several more on hand in case a need arises. The company no longer has to store old workstations and repurpose them as a need arises, which is always an immediate need.

Case 2 utilizes virtualization but has also incorporated the remaining components of cloud functionality. The services can be accessed either by VPN connection via the Internet or by an secure socket layer (SSL)/transport layer security (TLS) web-based portal. Management and IT are able to monitor and track the actual usage of each service by department or as granular as a monthly or hourly basis. Most importantly, upper-level IT resources are freed up as local IT staff, and delegated employees are able to add capacity as well as turn off machines. Once virtualization is paired with the five essential features listed earlier, true cloud services provide specific benefits to both the IT departments and consumers alike.

1.5 PRIVATE CLOUD AND VIRTUALIZATION

Case 1 displays the use of automation, server consolidation, and a service-oriented architecture. Although case 1 alone does not represent a cloud deployment, it necessitates some of the core impressions of cloud computing. Therefore, not all virtualized environments are private clouds.

When an organization requires a secure environment due to regulatory governance, private cloud addresses security concerns by accessing VPNs, having physical environments, or incorporating both types within the firewall. Health care and pharmaceutical companies require their data and applications to conform to a mixture of regulatory standards. Therefore, transferring sensitive data to the cloud violates privacy specifications. Private cloud deployments are desirable in such cases as both a segregated and physical location has the flexibility and capability to be fluid with workloads among servers as usage increases or as new applications are deployed.

1.6 COMMUNITY CLOUD

Community clouds offer similar advantages of a private cloud deployment, but at a lower cost and greater flexibility. The infrastructure can reside either on- or off-premise and can be managed either by the organization or by a service provider. As shown in Figure 1.6 [3],

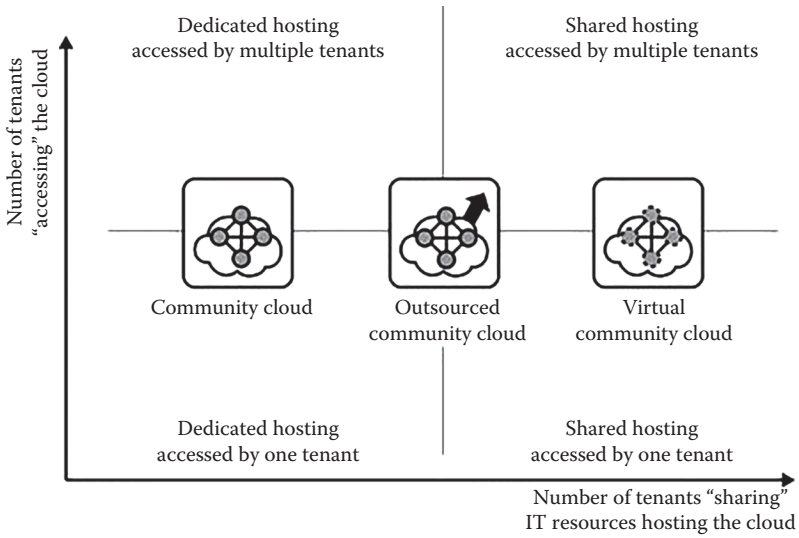

FIGURE 1.6 Whenever companies collaborate, they commonly have access to shared application and data to do business. Even though the companies have mutual relationships and agreements in place, the data and application functionality may be sensitive and critical to their business needs.

multitenancy is the key attribute to community cloud; it shares multiple services of the cloud service models: IaaS, PaaS, and SaaS. Technology organizations and their clients often collaborate and work on shared projects and applications. A central cloud computing service is essential when executing this type of project; thus, community cloud is an ideal solution. Data security, compliance, and policy considerations are all taken into consideration and accounted for when data are shared with others in the community and controlled in a secure fashion. Even though a community cloud is a more secure option than the public cloud, exercise discretion when storing data because it is accessible to everyone in the community. Proper allocation of governance and security must be instituted and still poses challenges in community cloud deployments.

1.7 HYBRID CLOUD

Hybrid cloud computing can be used as a stepping stone to mainstream cloud computing, as it involves the aggregation of cloud services utilizing two or more clouds, (private, community, and public). Of all service models, hybrid cloud features the most efficiency, best performance, reduced risk, and most granular customization. Organizations have the most control of their data even though this is a cloud model. Most businesses adopting the hybrid cloud model continue to run a business critical core application in-house; and, are running all other applications in the cloud, all the while in control of their secret sauce. Figure 1.7 shows a hybrid cloud environment.

Companies who are not ready to store their applications or files in the cloud for access can back up data to the cloud. One of the most popular uses of hybrid cloud computing is disaster recovery. Business continuity planning minimizes downtime with the ability to have an entire working environment operational in a very short period of time.

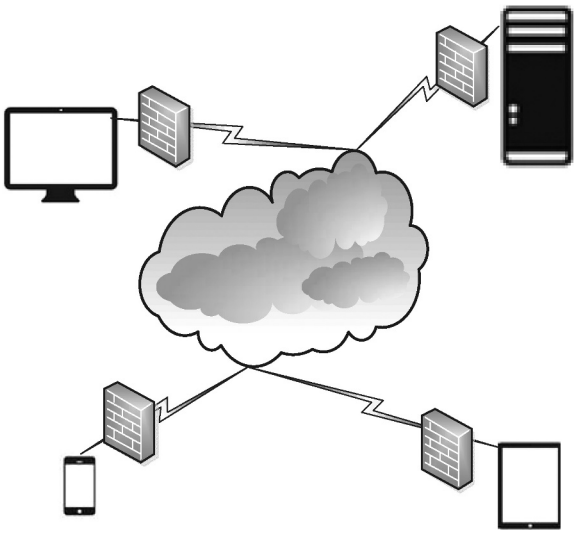

FIGURE 1.7 Hybrid cloud computing environments are device agnostic and all connect to the cloud securely.

1.8 SUMMARY

The cloud market is offering multiple options for businesses to transition their infrastructure, development platform, storage, and software. True innovation comes when successfully navigating the cloud space from traditional on-premise models to a recurring revenue model. Service providers are offering hybrid, private, and public cloud solutions, which lead to better efficiency, self-service, manipulation, and variety.

REFERENCES

1. Mell, Peter M., and Timothy Grance. *Publication Citation: The NIST Definition of Cloud Computing*. The National Institute of Standards and Technology, December 19, 2013. Web. April 23, 2015.
2. Brown, Evelyn. *Final Version of NIST Cloud Computing Definition Published*. Web. May 9, 2015.
3. "Community Cloud." *Cloud Computing Patterns*, n.d. Web. June 30, 2015.

References

1 Chapter 1: Private Cloud Computing Essentials

1. Mell, Peter M., and Timothy Grance. Publication Citation: The NIST Definition of Cloud Computing. The National Institute of Standards and Technology, December 19, 2013. Web. April 23, 2015.

2. Brown, Evelyn. Final Version of NIST Cloud Computing Definition Published. Web. May 9, 2015.

3. “Community Cloud.” Cloud Computing Patterns, n.d. Web. June 30, 2015.

FIGURE 1.7 Hybrid cloud computing environments are device agnostic and all connect to the

cloud securely.

2 Chapter 2: Integration of Enterprise Content Management and Software as a Service

1. AIIM Glossary. What Is Enterprise Content Management (ECM)? Association for Information and Image Management, Silver Spring, MD, 2015.

2. Gartner IT Glossary. Integration Platform as a Service (iPaaS). Gartner, Stamford, CT, 2015.

3. Badger, Lee, Tim Grance, Robert Patt-Comer, and Je Voas. Cloud Computing Synopsis and Recommendations. Gathersburg, MD: National Institute of Standards and Technology, 2012.

4. InterPARES Trust. Terminology Database [Restricted access]. interparestrust.org, 2015.

5. ANSI/AIIM/ARMA. Revised Framework for the Integration of Electronic Document Management Systems and Electronic Records Management Systems. Silver Springs, MD: AIIM ® , 2006.

6. Infosys. An ECM Journey [White paper]. infosys.com, 2014.

7. Hullavard, Shiva, Russell O'Hare, and Ashok K. Roy. Enterprise Content Management solutions—Roadmap strategy and implementation challenges. International Journal of Information Management, 35: 260–265, 2015.

8. Gilbert, Mark R., Karen M. Shegda, Kenneth Chin, Gavin Tay, and Hanns Koehler-Kruener. Gartner: Magic Quadrant for Enterprise Content Management. Gartner.com., 2015.

9. Nucleus Research. Technology Value Matrix 2015: ECM, 2015.

10. DATAMARK. Organizations Struggling to Implement Mobile Enterprise Content Management (ECM). DATAMARK, 2015.

11. DATAMARK. AIIM: e Era of Enterprise Content Management (ECM) is coming to an end. Outsourcing News, 2015.

12. Mann, Je rey and Bill Pray. Office 365, Google Apps for Work and Other Cloud Office Key Initiative Overview. Gartner, Stamford, CT, 2015.

13. Microso . Office 365 Trust Center. Microso O ce 365, 2015.

14. Google. Google Apps for Work. Get Email for Your Business. Google, n.d.

15. Ponemon Institute. Achieving Security in Workplace File Sharing. Ponemon Institute LLC, 2014.

16. Desisto, Robert P. and Tad Travis. Magic Quadrant for Sales Force Automation. Gartner, 2015.

17. SNIA. The 2015 SNIA Dictionary. SNIA, 2015.

18. Franks, Patricia. Records and Information Management, pp. 280-282. Chicago, IL: ALANeal-Schuman, 2013.

19. International Organization for Standardization (ISO). ISO standard 14721: 2012, Space data and information transfer systems—Open archival information system (OAIS)—International Organization for Standardization (ISO). Reference model, 2nd edition, pp. 1-2. Geneva, Switzerland: ISO, 2012.

20. Franks, Patricia C. Government Use of cloud-based long term digital preservation as a service: An exploratory study. Proceedings of the 2nd Digital Heritage International Congress, 2015.

21. Association for Information and Image Management (AIIM). ECM at the Crossroads, p. 4. AIIM, 2013.

22. Trebaol, Lacey. Integration vs. interoperation. Real-Time Innovations Blog, 2013.

23. Microso. System requirements for O ce. Microsoft Office, 2015.

24. EMC. Documentum by EMC. EMC 2 , 2015.

25. EMC. Documentum Connector for Microso SharePoint. EMC 2 , 2015.

26. Pezzini, Massimo, Ye m V. Natis, Paolo Malinverno, Kimihiko Iijima, Jess ompson, Eric oo, and Keith Guttridge. Magic Quadrant for Enterprise Integration Platform as a Service, Worldwide. Gartner, 2015.

27. Cisco. Seize New IoT Opportunities with the Cisco IoT System. Cisco, n.d.

28. Microso. Azure IoT Suite now available. Microsoft,

Internet of Things, 2015.

29. General Electric. GE Announces Predix Cloud—The World's First Cloud Service Built for Industrial Data and Analytics [Press release], 2015.

3 Chapter 3: Infrastructure as a Service

1. Gurkok, Cem. Securing Cloud Computing Systems. In Vacca, J. R., ed. Computer and Information Security Handbook. 2nd Edition. Elsevier: Boston, MA, 2013, pp. 97-123.

2. National Institute of Standards and Technology. The NIST Definition of Cloud Computing. NIST Special Publication Gaithersburg, MD, 2011, 800-145.

3. Yeluri, Raghu and Enrique Castro-Leon. Building the Infrastructure for Cloud Security. Apress Media: New York, 2014, pp. 160-163.

4 Chapter 4: Preservation as a Service for Trust

Delauney, Jean-Yves. 2012. “Overview of the LOTAR Project and LOTAR Standards, Status of Implementation in Europe.” Presented at the GIFAS, Paris, France, May 29. http://www.lotar-international.org/fileadmin/user_upload/documents/2_2012-05-29_GIFAS_LOTAR_Overview_Final_V5.pdf#page=30&zoom=auto,-106,30.

Duranti, Luciana, and Kenneth Ribodeau. 2006. “The Concept of Record in Interactive, Experiential and Dynamic Environments: The View of InterPARES.” Archival Science 6 (1): 13–68.

Health Level Seven International. 2015. “Introduction to HL7 Standards.” Accessed September 13, 2015. http://www.hl7.org/implement/standards/.

Hockx-Yu, Helen, and Gareth Knight. 2008. “What to Preserve?: Signi□cant Properties of Digital Objects.” The International Journal of Digital Curation 3 (1): 141–153.

International Organization for Standardization. 2015. “ISO 14721:2012—Space Data and Information Transfer Systems—Open Archival Information System (OAIS)—Reference Model.” Accessed September 13, 2015. http://www.iso.org/iso/catalogue_detail.htm?csnumber=57284.

InterPARES. 2015. “InterPARES 2 Project: Terminology Database.” Accessed September 13, 2015. http://interpares.org/ip2/ip2_terminology_db.cfm.

ISO/IEC Joint Technical Committee. 2015. “Text of ISO/IEC DIS 23000-15 Multimedia Preservation Application Format | MPEG.” February 20. http://mpeg.chiariglione.org/standards/mpeg-a/

Matthews, Brian, Juan Bicarregui, Arif Shaon, and Catherine Jones. 2009. “Framework for So□ware Preservation.” Report. Accessed September 13, 2015. https://epubs.stfc.ac.uk/work/51076.

NIST, Interagency Working Group on Digital Data. 2009. “Harnessing the Power of Digital Data for Science and Society.” Report of the Interagency Working Group on Digital Data to the Committee on Science of the National Science and Technology Council. Accessed September 13, 2015.

Norsam Technologies. 2015. “HD-Rosetta TM and Related Processes.” Accessed September 13, 2015. http://www.norsam.com/rosetta.html.

Object Management Group. 2011. “Records Management Services (RMS), Version 1.0.” Accessed September 13, 2015. http://www.omg.org/spec/RMS/1.0.

O□ce of the Law Revision Counsel. 2015. “United States Code, Title 44.” Accessed September 13, 2015.

Schi□, Jennifer. 2008. “Storage □at Really Lasts.” September 11. Accessed September 13, 2015.

Simmhan, Yogesh L, Beth Plale, and Dennis Gannon. 2005. “A Survey of Data Provenance in E-Science.” SIGMOD Record 34 (3): 31–36.

World Wide Web Consortium. 2015. “Extensible Markup Language (XML).” September 5. Accessed September 13, 2015. http://www.w3.org/XML/.

XBRL International. 2013. “Extensible Business Reporting Language (XBRL) 2.1.” February 20. Accessed September 13, 2015. http://www.xbrl.org/Speci□cation/XBRL-2.1/REC-2003-12-31/XBRL-2.1-REC-2003-12-31+corrected-errata-2013-02-20.html.

5 Chapter 5: Software and Data Segregation Security

Carroll, M., Van Der Merwe, A., and Kotze, P. (2011). Secure Cloud Computing: Benefits, Risks and Controls. Paper presented at the Information Security South Africa (ISSA).

Chaves, D., Aparecida, S., Uriarte, R. B., and Westphall, C. B. (2011). Toward an architecture for monitoring private clouds. Communications Magazine, IEEE, 49(12), 130–137.

Chen, D., and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. Paper presented at the International Conference on Computer Science and Electronics Engineering (ICCSEE).

Dillon, T., Wu, C., and Chang, E. (2010). Cloud Computing: Issues and Challenges. Paper presented at the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA).

Doelitzscher, F., Sulistio, A., Reich, C., Kuijs, H., and Wolf, D. (2011). Private cloud for collaboration and e-learning services: From IaaS to SaaS. Computing, 91(1), 23–42.

Domingo, E. J., Niño, J. T., Lemos, A. L., Lemos, M. L., Palacios, R. C., and Berbís, J. M. G. (2010). CLOUDIO: A Cloud Computing-Oriented Multi-Tenant Architecture for Business Information Systems. Paper presented at the IEEE 3rd International Conference on Cloud Computing (Cloud).

Dustin Owens, B. (2010). Securing elasticity in the cloud. Communications of the ACM, 53(6).

Foster, I., Zhao, Y., Raicu, I., and Lu, S. (2008). Cloud Computing and Grid Computing 360-Degree Compared. Paper presented at the Grid Computing Environments Workshop.

Géczy, P., Izumi, N., and Hasida, K. (2013). Hybrid cloud management: Foundations and strategies. Review of Business and Finance Studies, 4(1), 37–50.

Hashizume, K., Rosado, D. G., Fernández-Medina, E., and Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 1–13.

Malathi, M. (2011). Cloud Computing Concepts. Paper presented at the 3rd International Conference on Electronics Computer Technology.

Mather, T., Kumaraswamy, S., and Latif, S. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media.

Mehrsai, A., Karimi, H. R., and □oben, K.-D. (2013). Integration of supply networks for customization with modularity in cloud and make-to-upgrade strategy. Systems Science and Control Engineering: An Open Access Journal, 1(1), 28-42.

Popa, L., Kumar, G., Chowdhury, M., Krishnamurthy, A., Ratnasamy, S., and Stoica, I. (2012). FairCloud: Sharing the Network in Cloud Computing. Paper presented at the Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication.

Sotola, R. (2011). Billing in the cloud: □e missing link for cloud providers. Journal of Telecommunications Management, 3(4).

Wood, T., Ramakrishnan, K., Shenoy, P., and Van der Merwe, J. (2011). CloudNet: Dynamic Pooling of Cloud Resources by Live WAN Migration of Virtual Machines. Paper presented at the ACM SIGPLAN Notices.

Zhang, Q., Cheng, L., and Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7-18.

6 Chapter 6: Taking Full Responsibility for Cyber Security in the Private Cloud

Abu Rajab, M., Zarfoss, J., Monrose, F., and Terzis, A. (2006). A multifaceted approach to understanding the botnet phenomenon. Paper presented at the Proceedings of the 6th ACM SIGCOMM conference on Internet measurement.

Alrwais, S. A., Gerber, A., Dunn, C. W., Spatscheck, O., Gupta, M., and Osterweil, E. (2012). Dissecting ghost clicks: Ad fraud via misdirected human clicks. Paper presented at the Proceedings of the 28th Annual Computer Security Applications Conference.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies and Management, 29(3), 408–433.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., and Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime. International Journal of Cyber Criminology, 8(1), 1–20.

Cache, J., Wright, J., Liu, V., Scott, E., Antoniewiecz, B., and Wang, C. (2010). Hacking Exposed Wireless. McGraw-Hill.

Chen, H., Chung, W., Xu, J. J., Wang, G., Qin, Y., and Chau, M. (2004). Crime data mining: A general framework and some examples. Computer, 37(4), 50–56.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers and Security, 30(8), 719–731.

Duijn, P. A., Kashirin, V., and Sloot, P. M. (2014). The relative ineffectiveness of criminal network disruption. Scientific reports, 4.

Florêncio, D., and Herley, C. (2013). Sex, lies and cyber-crime surveys. In Economics of Information Security and Privacy III (pp. 35–53). Springer.

Gad, M. (2014). Crimeware marketplaces and their facilitating technologies. Technology Innovation Management Review, 4(11).

Greenwald, G., MacAskill, E., and Poitras, L. (2013). Edward Snowden: The whistleblower behind the NSA

surveillance revelations. The Guardian, 9.

Håpnes, T., and Sørensen, K. H. (1995). Competition and collaboration in male shaping of computing: A study of a Norwegian hacker culture. The Gender-Technology Relation: Contemporary Theory and Research, 174-191.

Kasar, S. (2006). Legal issues alone are not enough to manage computer fraud committed by employees. Journal of International Commercial Law and Technolgy, 1, 25.

Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., and Lee, B. S. (2011). TrustCloud: A framework for accountability and trust in cloud computing. Paper presented at the 2011 IEEE World Congress on Services (SERVICES).

Marshall, B., Kaza, S., Xu, J., Atabakhsh, H., Petersen, T., Violette, C., and Chen, H. (2004). Crossjurisdictional criminal activity networks to support border and transportation security. Paper presented at the Proceedings of the 7th International IEEE Conference on Intelligent Transportation Systems.

McCoy, D., Bauer, K., Grunwald, D., Kohno, T., and Sicker, D. (2008). Shining light in dark places: Understanding the Tor network. Paper presented at the Privacy Enhancing Technologies.

Mera, A. (2015). Unintentional insider threat: Policy, training and technologies to mitigate end user risk.

Rebollo, O., Mellado, D., and Fernández-Medina, E. (2012). A systematic review of information security governance frameworks in the cloud computing environment. Jouranl of Universal Computer Science, 18(6), 798-815.

Wall, D. (2007). Cybercrime: The Transformation of Crime in the Information Age (Vol. 4). Polity.

Walters, R. (2014). Cyber attacks on US companies in 2014. Heritage Foundation Issue Brief (4289).

Yang, D. W., and Ho□stadt, B. M. (2006). Countering the cyber-crime threat. American Criminal Law Review, 43, 201.

7 Chapter 7: Selecting the Appropriate Product

Armbrust, M., Fox, A., Gri□th, R., Joseph, A. D., Katz, R., Konwinski, A., … Stoica, I. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

Bardin, J., Callas, J., Chaput, S., Fusco, P., Gilbert, F., Ho□, C., … Matsumoto, S. (2009). Security guidance for critical areas of focus in cloud computing. Cloud Security Alliance, 0-176.

Buhalis, D., and Law, R. (2008). Progress in information technology and tourism management: 20 years on and 10 years a□er the Internet—□e state of eTourism research. Tourism Management, 29(4), 609-623.

De Haes, S., and Van Grembergen, W. (2005). IT governance structures, processes and relational mechanisms: Achieving IT/business alignment in a major Belgian □nancial group. Paper presented at the Proceedings of the 38th Annual Hawaii International Conference on System Sciences, 2005.

Durkee, D. (2010). Why cloud computing will never be free. Queue, 8(4), 20.

Feuerlicht, G., Burkon, L., and Sebesta, M. (2011). Cloud computing adoption: What are the issues. Systémová Integrace, 187-192.

Guo, Z., Song, M., and Song, J. (2010). Notice of retraction a governance model for cloud computing. Paper presented at the 2010 International Conference on Management and Service Science (MASS).

Harris, S., Harper, A., Ness, J., Williams, T., and Lenkey, G. (2011). Gray hat hacking.

Kaminsky, D. (2006). Explorations in namespace: White-hat hacking across the domain name system. Communications of the ACM, 49(6), 62-69.

Kandukuri, B. R., Paturi, V. R., and Rakshit, A. (2009). Cloud security issues. Paper presented at the IEEE International Conference on Services Computing, 2009.
Viruses, Trojan horses, and worms Social engineering Automated attacks Accidental breaches in security Denial of service Organizational attacks Restricted data

FIGURE 7.6 Scope of white hacking.

Kégl, B., Krzyzak, A., Linder, T., and Zeger, K. (2000). Learning and design of principal curves. IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(3), 281–297.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., and Ghalsasi, A. (2011). Cloud computing—Ꭾe business perspective. Decision Support Systems, 51(1), 176–189.

Mell, P., and Grance, T. (2011). Ꭾe NIST deꭾnition of cloud computing.

Ness, R. B., and Joint Policy Committee (2007). Inꭾuenceꭾofꭾthe HIPAA privacy rule on health research. JAMA, 298(18), 2164–2170.

Sądowski, A., Narayan, R., Sironi, L., and Özel, F. (2013). Location of the bow shock ahead of cloud G2 at the Galactic Centre. Monthly Notices of the Royal Astronomical Society, 433(3), 2165–2171.

Sistanizadeh, K., Amin-Salehi, B., Ghafari, E., and Sims, W. (2002). Universal access multimedia data network. Google Patents.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. (2005). Analysis of end user security behaviors. Computers and Security, 24(2), 124–133.

Walker, E., Brisken, W., and Romney, J. (2010). To lease or not to lease from storage clouds. Computer, 43(4), 44–50.

Wan, Z., Liu, J. E., and Deng, R. H. (2012). HASBE: A hierarchical attribute-based solution for ꭾexible and scalable access control in cloud computing. IEEE Transactions on Information Forensics and Security, 7(2), 743–754.

Wang, C., Wang, Q., Ren, K., and Lou, W. (2010). Privacy-preserving public auditing for data storage security in cloud computing. Paper presented at the 2010 Proceedings IEEE on INFOCOM.

Zhao, G.-S., Rong, C.-M., Liu, J.-L., Liu, H., Zhang, F., Ye, X.-P., … Tang, Y. (2010). Modeling user growth for cloud scalability and availability. Journal of Internet Technology, 11(3), 395–405.

9 Chapter 9: Security in the Virtual Private Cloud

Ahmed, M., Chowdhury, A., Ahmed, M., & Rafee, M. M. H. (2012). An advanced survey on cloud computing and state-of-the-art research issues. IJCSI International Journal of Computer Science Issues, 9(1), 1694-0814.

Beach, B. (2014). Virtual Private Cloud. In Pro Powershell for Amazon Web Services (pp. 67-88). Springer.

Chaves, D., Aparecida, S., Uriarte, R. B., & Westphall, C. B. (2011). Toward an architecture for monitoring private clouds. IEEE Communications Magazine, 49(12), 130-137.

Doelitzscher, F., Sulistio, A., Reich, C., Kuijs, H., & Wolf, D. (2011). Private cloud for collaboration and e-Learning services: From IaaS to SaaS. Computing, 91(1), 23-42.

Durkee, D. (2010). Why cloud computing will never be free. Queue, 8(4), 20.

Jadeja, Y., & Modi, K. (2012). Cloud computing-concepts, architecture and challenges. Paper presented at the 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET).

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. NIST Special Publication, 800, 144.

Keahey, K., Figueiredo, R., Fortes, J., Freeman, T., & Tsugawa, M. (2008). Science clouds: Early experiences in cloud computing for scienti□c applications. Cloud Computing and Applications, 2008, 825-830.

Krautheim, F. J. (2009). Private virtual infrastructure for cloud computing. Proceedings of HotCloud.

Lee, K. (2012). Security threats in cloud computing environments. International Journal of Security and Its Applications, 6(4), 25-32.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—□e business perspective. Decision Support Systems, 51(1), 176-189.

Mell, P., & Grance, T. (2011). □e NIST de□nition of cloud computing.

Moghaddam, F. F., Cheriet, M., & Nguyen, K. K. (2011). Low carbon virtual private clouds. Paper presented at the 2011 IEEE International Conference on Cloud Computing (CLOUD).

Porwal, A., Maheshwari, R., Pal, B., & Kakhani, G. (2012). An approach for secure data transmission in private cloud. International Journal of Soft Computing and Engineering (IJSCE) ISSN, 2231-2307.

Sabahi, F. (2011). Cloud computing security threats and responses. Paper presented at the 2011 IEEE 3rd International Conference on Communication So□ware and Networks (ICCSN).

Sotomayor, B., Montero, R. S., Llorente, I. M., & Foster, I. (2009). Virtual infrastructure management in private and hybrid clouds. IEEE Internet Computing, 13(5), 14-22.

Wood, T., Gerber, A., Ramakrishnan, K., Shenoy, P., & Van der Merwe, J. (2009). □e case for enterprise-ready virtual private clouds. Usenix HotCloud.

10 Chapter 10: The Hybrid Cloud Alternative

Flores, H., Srirama, S. N., and Paniagua, C. (2011). A generic middleware framework for handling process intensive hybrid cloud services from mobiles. Paper presented at the Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia.

Gĕczy, P., Izumi, N., and Hasida, K. (2013). Hybrid cloud management: Foundations and strategies. Review of Business and Finance Studies, 4(1), 37-50.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013). Internet of ﬁngs (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

Li, Q., Wang, Z.-y., Li, W.-h., Li, J., Wang, C., and Du, R.-y. (2013). Applications integration in a hybrid cloud computing environment: Modelling and platform. Enterprise Information Systems, 7(3), 237-271.

Mell, P., and Grance, T. (2009). Eﬀectively and securely using the cloud computing paradigm. NIST, Information Technology Laboratory, 304-311.

Mell, P., and Grance, T. (2011). ﬀe NIST deﬁnition of cloud computing.

Ramgovind, S., Eloﬀ, M. M., and Smith, E. (2010). ﬀe management of security in cloud computing. Paper presented at the Information Security for South Africa (ISSA).

Sefraoui, O., Aissaoui, M., and Eleuldj, M. (2012). OpenStack: Toward an open-source solution for cloud computing. International Journal of Computer Applications, 55(3), 38-42.

Seshadri, A., Luk, M., Qu, N., and Perrig, A. (2007). SecVisor: A tiny hypervisor to provide lifetime kernel code integrity for commodity OSes. ACM SIGOPS Operating Systems Review, 41(6), 335-350.

Sotomayor, B., Montero, R. S., Llorente, I. M., and Foster, I. (2009). Virtual infrastructure management in private and hybrid clouds. IEEE Internet Computing, 13(5), 14-22.

Suresh, K., and Prasad, K. (2012). Security issues and security algorithms in cloud computing. International

Journal of Advanced Research in Computer Science and Software Engineering, 2(10).

Witt III, W. F. (2010). Keep your feet on the ground when moving so□ware into the cloud. JDCTA, 4(2), 10-17.

11 Chapter 11: Identification and Privacy in the Secure Cloud

1. Burr, William et al., NIST Special Publication 800-63-2 Electronic Authentication Guideline, NIST, 2013.

2. Jansen, Wayne and Grance, Timothy, NIST Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing, NIST, 2011.

12 Chapter 12: Private Cloud Security and Identification

Alperin-Sheri, J., and Peikert, C. (2014). Faster bootstrapping with polynomial error. In Advances in Cryptology—CRYPTO 2014 (pp. 297-314). Springer.

Atayero, A. A., and Feyisetan, O. (2011). Security issues in cloud computing: e potentials of homomorphic encryption. Journal of Emerging Trends in Computing and Information Sciences, 2(10), 546-552.

Bailey, D. V., and Paar, C. (2001). E cient arithmetic in nite eld extensions with application in elliptic curve cryptography. Journal of Cryptology, 14(3), 153-176.

Bausch, P. (2003). Amazon Hacks. O'Reilly Media, Inc.

Beloglazov, A., Piraghaj, S. F., Alrokayan, M., and Buyya, R. (2012). Deploying OpenStack on CentOS Using the KVM Hypervisor and GlusterFS distributed file system. Cloud Computing and Distributed Systems (CLOUDS) Laboratory Department of Computing and Information Systems, e University of Melbourne, Australia.

Bertino, E., Paci, F., Ferrini, R., and Shang, N. (2009). Privacy-preserving digital identity management for cloud computing. IEEE Data Engineering Bulletin, 32(1), 21-27.

Brenner, M., Wiebelitz, J., Von Voigt, G., and Smith, M. (2011). Secret program execution in the cloud applying homomorphic encryption. Paper presented at the 2011 Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies Conference.

Brinkman, R. (2007). Searching in Encrypted Data. University of Twente.

Chisnall, D. (2008). The Definitive Guide to the Xen Hypervisor. Pearson Education.

Chun, B.-G., Ihm, S., Maniatis, P., Naik, M., and Patti, A. (2011). Clonecloud: Elastic execution between mobile device and cloud. Paper presented at the Proceedings of the Sixth Conference on Computer Systems.

Coglianese, M., and Goi, B.-M. (2005). MaTRU: A new NTRU-based cryptosystem. In Progress in Cryptology-INDOCRYPT 2005 (pp. 232-243). Springer.

Coron, J.-S., Lepoint, T., and Tibouchi, M. (2014). Scale-invariant fully homomorphic encryption over the integers. In Public-Key Cryptography–PKC 2014 (pp. 311–328). Springer.

Cramer, R., Damgård, I., and Nielsen, J. B. (2001). Multiparty Computation from Threshold Homomorphic Encryption. Springer.

Dixon, B., and Lenstra, A. K. (1993). Massively parallel elliptic curve factoring. Paper presented at the Advances in Cryptology—EUROCRYPT'92.

Fujisaki, E., and Okamoto, T. (1999). Secure integration of asymmetric and symmetric encryption schemes. Paper presented at the Crypto.

Gampala, V., Inuganti, S., and Muppidi, S. (2012). Data security in cloud computing with elliptic curve cryptography. International Journal of Soft Computing and Engineering, 2(3), 138–141.

Gedik, B., and Liu, L. (2005). Location privacy in mobile systems: A personalized anonymization model. Paper presented at the Proceedings of the 25th IEEE International Conference on Distributed Computing Systems.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. Paper presented at the STOC.

Gentry, C. (2010). Computing arbitrary functions of encrypted data. Communications of the ACM, 53(3), 97–105.

Gentry, C., Halevi, S., and Smart, N. P. (2012). Homomorphic evaluation of the AES circuit. In Advances in Cryptology—CRYPTO 2012 (pp. 850–867). Springer.

Gura, N., Patel, A., Wander, A., Eberle, H., and Shantz, S. C. (2004). Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In Cryptographic Hardware and Embedded Systems-CHES 2004 (pp. 119–132). Springer.

Hankerson, D., and Menezes, A. (2011). Elliptic curve discrete logarithm problem. In Encyclopedia of Cryptography and Security (pp. 397–400). Springer.

Hankerson, D., Menezes, A. J., and Vanstone, S. (2006). Guide to Elliptic Curve Cryptography. Springer Science+Business Media.

He, Y., and Naughton, J. F. (2009). Anonymization of set-valued data via top-down, local generalization. Proceedings of the VLDB Endowment, 2(1), 934-945.

Herzog, J. C. (2003). The Diffie-Hellman key-agreement scheme in the strand-space model. Paper presented at the Proceedings of the 16th IEEE on Computer Security Foundations Workshop.

Jansen, W. (2011). Cloud hooks: Security and privacy issues in cloud computing. Paper presented at the 2011 44th Hawaii International Conference on System Sciences.

Lauter, K. (2004). The advantages of elliptic curve cryptography for wireless security. IEEE Wireless Communications, 11(1), 62-67.

Law, L., and Solinas, J. (2007). Suite B cryptographic suites for IPsec.

Lawson, J., Wolthuis, J., and Cooke, E. (2010). System and method for mitigating a denial of service attack using cloud computing. Google Patents.

Lee, B., Kim, H., and Kim, K. (2001). Strong proxy signature and its applications. Paper presented at the Proceedings of SCIS.

Liu, A., and Ning, P. (2008). TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. Paper presented at the International Conference on Information Processing in Sensor Networks.

Micciancio, D. (2010). A first glimpse of cryptography's Holy Grail. Communications of the ACM, 53(3), 96-96.

Nergiz, M. E., Clifton, C., and Nergiz, A. E. (2009). Multirelational k-anonymity. IEEE Transactions on Knowledge and Data Engineering, 21(8), 1104-1117.

Olden, E. (2011). Architecting a cloud-scale identity fabric. Computer, 44(3), 52-59.

Oliveira, S. R. (2003). Protecting sensitive knowledge by data sanitization. Paper presented at the null.

Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. Paper presented at the Advances in Cryptology—EUROCRYPT'99.

Palankar, M. R., Iamnitchi, A., Ripeanu, M., and Garﬁnkel, S. (2008). Amazon S3 for science grids: A viable solution? Paper presented at the Proceedings of the 2008 International Workshop on Data-Aware Distributed Computing.

Shiller, R. J. (2009). The New Financial Order: Risk in the 21st Century. Princeton University Press.

Stehlé, D., and Steinfeld, R. (2010). Faster fully homomorphic encryption. In Advances in Cryptology—ASIACRYPT 2010 (pp. 377–394). Springer.

Sweeney, L. (2002). k-Anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), 557–570.

Vasudevan, A., Chaki, S., Jia, L., McCune, J., Newsome, J., and Datta, A. (2013). Design, implementation and verification of an extensible and modular hypervisor framework. Paper presented at the 2013 IEEE Symposium on Security and Privacy.

Wahbe, R., Lucco, S., Anderson, T. E., and Graham, S. L. (1994). Efficient software-based fault isolation. Paper presented at the ACM SIGOPS Operating Systems Review.

13 Chapter 13: Secure Management of Virtualized Resources

1. Wylve and Bikeborg. Cloud computing layers. Wikimedia Foundation, Inc.: San Francisco, CA.

2. Jongse Park, Daewoo Lee, Bokyeong Kim, Jaehyuk Huh, and Seungryoul Maeng. Localityaware dynamic VM recon□guration on map reduce clouds. In Proceedings of the 21st International Symposium on High-Performance Parallel and Distributed Computing, pp. 27–36, ACM: New York, 2012.

3. Khalid Bijon, Ram Krishnan, and Ravi Sandhu. Mitigating multi-tenancy risks in IaaS cloud through constraints-driven virtual resource scheduling. In Proceedings of the 20th ACM Symposium on Access Control Models and Technologies, pp. 63–74, ACM: New York, 2015.

4. KhalidZaman Bijon, Ram Krishnan, and Ravi Sandhu. A formal model for isolation management in cloud infrastructure-as-a-service. In ManHo Au, Barbara Carminati, and C.-C. Jay Kuo, editors, Network and System Security, volume 8792 of Lecture Notes in Computer Science, pp. 41–53, Springer International Publishing, 2014.

5. Khalid Bijon, Ram Krishnan, and Ravi Sandhu. Virtual resource orchestration constraints in cloud infrastructure as a service. In Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, pp. 183–194, ACM: New York, 2015.

6. □omas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. Hey, you, get o□ of my cloud: Exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 199–212, ACM: New York, 2009.

7. Venkatanathan Varadarajan, □awan Kooburat, Benjamin Farley, □omas Ristenpart, and Michael M. Swi□. Resource-freeing attacks: Improve your cloud performance (at your neighbor’s expense). In Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 281–292, ACM: New York, 2012.

8. Yinqian Zhang, Ari Juels, Michael K. Reiter, and □omas Ristenpart. Cross-VM side channels and their use to extract private keys. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 305–316, ACM: New York, 2012.

9. Yinqian Zhang, Ari Juels, Michael K. Reiter, and Thomas Ristenpart. Cross-tenant side- channel attacks in PaaS clouds. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 990–1003, ACM: New York, 2014.

10. T. Takahashi, G. Blanc, Y. Kadobayashi, D. Fall, H. Hazeyama, and S. Matsuo. Enabling secure multitenancy in cloud computing: Challenges and approaches. In 2012 2nd Baltic Congress on Future Internet Communications (BCFIC), pp. 72–79, 2012.

11. G. C. Deka. Cost-benefit analysis of datacenter consolidation using virtualization. IT Professional, 16(6):54–62, 2014.

12. M. Caliskan, M. Ozsiginan, and E. Kugu. Benefits of the virtualization technologies with intrusion detection and prevention systems. In 2013 7th International Conference on Application of Information and Communication Technologies (AICT), pp. 1–5, 2013.

13. G. Minutoli and A. Puliafito. GliteVM: How science and business may benefit from virtualization. In Eighth IEEE International Symposium on Network Computing and Applications, 2009, pp. 126–129, 2009.

14. Edward Ray and Eugene Schultz. Virtualization security. In Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, pp. 42:1–42:5, ACM: New York, 2009.

15. S.T. King and P.M. Chen. Subvirt: Implementing malware with virtual machines. In 2006 IEEE Symposium on Security and Privacy, pp. 14–327, 2006.

16. Gefner Jason. VENOM: Virtualized Environment Neglected Operations Manipulation. http://venom.crowdstrike.com/, May 2015. [Online].

17. John Scott Robin and Cynthia E. Irvine. Analysis of the Intel Pentium's ability to support a secure virtual machine monitor. In Proceedings of the 9th Conference on USENIX Security Symposium—Volume 9, pp. 10–10, USENIX Association: Berkeley, CA, 2000.

18. David Carrera, Malgorzata Steinder, Ian Whalley, Jordi Torres, and Eduard Ayguadé. Enabling resource sharing between transactional and batch workloads using dynamic

application placement. In Proceedings of the 9th ACM/IFIP/USENIX International Conference on Middleware, pp. 203–222, 2008.

19. Jason Mars, Lingjia Tang, Robert Hundt, Kevin Skadron, and Mary Lou So▯a. Bubble-up: Increasing utilization in modern warehouse scale computers via sensible co-locations. In Proceedings of the 44th Annual IEEE/ACM International Symposium on Microarchitecture, pp. 248–259, 2011.

20. Ripal Nathuji, Aman Kansal, and Alireza Gha▯arkhah. Q-clouds: Managing performance interference e▯ects for QoS-aware clouds. In Proceedings of the 5th European Conference on Computer Systems, pp. 237–250. ACM: New York, 2010.

21. Xiaoyun Zhu, Don Young, B.J. Watson, Zhikui Wang, J. Rolia, S. Singhal, B. McKee, C. Hyser, D. Gmach, R. Gardner, T. Christian, and L. Cherkasova. 1000 islands: Integrated capacity and workload management for the next generation data center. In International Conference on Autonomic Computing, 2008, pp. 172–181, 2008.

22. Zhikui Wang, Yuan Chen, D. Gmach, S. Singhal, B.J. Watson, W. Rivera, Xiaoyun Zhu, and C.D. Hyser. Appraise: Application-level performance management in virtualized server environments. IEEE Transactions on Network and Service Management, 6(4):240–254, 2009.

23. Rui Wang and Nagarajan Kandasamy. A distributed control framework for performance management of virtualized computing environments: Some preliminary results. In Proceedings of the 1st Workshop on Automated Control for Datacenters and Clouds, pp. 7–12, 2009.

24. D. Minarolli and B. Freisleben. Utility-based resource allocation for virtual machines in cloud computing. In 2011 IEEE Symposium on Computers and Communications (ISCC), pp. 410–417, 2011.

25. Emerson Loureiro, Paddy Nixon, and Simon Dobson. A ne-grained model for adaptive ondemand provisioning of CPU shares in data centers. In Proceedings of the 3rd International Workshop on Self-Organizing Systems, pp. 97–108, 2008.

26. I. Goiri, Kien Le, M.E. Haque, R. Beauchea, T.D. Nguyen, J. Guitart, J. Torres, and R. Bianchini. Greenslot: Scheduling energy consumption in green datacenters. In 2011 International Conference for High

Performance Computing, Networking, Storage and Analysis (SC), pp. 1–11, 2011.

27. Yixin Diao and Aliza Heching. Closed loop performance management for service delivery systems. In 2012 IEEE Network Operations and Management Symposium, pp. 61–69, 2012.

28. Timothy Wood, Prashant Shenoy, Arun Venkataramani, and Mazin Yousif. Black-box and gray-box strategies for virtual machine migration. In Proceedings of the 4th USENIX Conference on Networked Systems Design and Implementation, pp. 17–17, 2007.

29. Akkarit Sangpetch, Andrew Turner, and Hyong Kim. How to tame your VMS: An automated control system for virtualized services. In Proceedings of the 24th International Conference on Large Installation System Administration, pp. 1–16, USENIX Association: Berkeley, CA, 2010.

30. O. Sukwong, A. Sangpetch, and H.S. Kim. Sageshi: Managing SLAs for highly consolidated cloud. In 2012 Proceedings of the IEEE INFOCOM, pp. 208–216, 2012.

31. Bin Lin and Peter A. Dinda. Vsched: Mixing batch and interactive virtual machines using periodic real-time scheduling. In Proceedings of the ACM/IEEE SC 2005, p. 8, 2005.

32. M. Kesavan, A. Ranadive, A. Gavrilovska, and K. Schwan. Active coordination (act)—Toward e ectively managing virtualized multicore clouds. In 2008 IEEE International Conference on Cluster Computing, pp. 23–32, 2008.

33. A. Gandhi, Yuan Chen, D. Gmach, M. Arlitt, and M. Marwah. Minimizing data center SLA violations and power consumption via hybrid resource provisioning. In Proceedings of the 2011 International Green Computing Conference and Workshops, pp. 1–8, IEEE Computer Society: Washington, DC, 2011.

34. Sergey Blagodurov, Daniel Gmach, Martin Arlitt, Yuan Chen, Chris Hyser, and Alexandra Fedorova. Maximizing server utilization while meeting critical SLAs via weight-based collocation management. In 2013 IFIP/IEEE International Symposium on Integrated Network Management, pp. 277–285, 2013.

35. Saad Rahim. State of GPU virtualization for cuda applications. Acceleware Ltd.: Calgary, Alberta, Canada.

http://acceleware.com/blog/
state-gpu-virtualization-cuda-applications-2014, 2014.

36. Micah Dowty and Jeremy Sugerman. GPU virtualization on vmware's hosted I/O architecture. SIGOPS Operating System Review, 43(3):73–82, 2009.

37. Lin Shi, Hao Chen, and Jianhua Sun. vCUDA: GPU accelerated high performance computing in virtual machines. In IEEE International Symposium on Parallel Distributed Processing, pp. 1–11, 2009.

38. Giulio Giunta, Ra□aele Montella, Giuseppe Agrillo, and Giuseppe Coviello. A GPGPU transparent virtualization component for high performance computing clouds. In Pasqua D'Ambra, Mario Guarracino, and Domenico Talia, editors, Euro-Par 2010—Parallel Processing, volume 6271 of Lecture Notes in Computer Science, pp. 379–391. Springer: Berlin, Germany, 2010.

39. J. Duato, A.J. Pena, F. Silla, R. Mayo, and Quintana-Orti E.S. rCUDA: Reducing the number of GPU-based accelerators in high performance clusters. In International Conference on High Performance Computing and Simulation, pp. 224–231, 2010.

40. Vishakha Gupta, Ada Gavrilovska, Karsten Schwan, Harshvardhan Kharche, Niraj Tolia, Vanish Talwar, and Parthasarathy Ranganathan. GViM: GPU-accelerated virtual machines. In Proceedings of the 3rd ACM Workshop on System-Level Virtualization for High Performance Computing, pp. 17–24, ACM: New York, 2009.

41. Shucai Xiao, P. Balaji, Qian Zhu, R. □akur, S. Coghlan, Heshan Lin, Gaojin Wen, Jue Hong, and Wu-chun Feng. VOCL: An optimized environment for transparent virtualization of graphics processing units. In Innovative Parallel Computing, pp. 1–12, 2012.

42. Clementine Maurice, Christoph Neumann, Olivier Heen, and Aurelien Francillon. Con□dentiality issues on a GPU in a virtualized environment. In Nicolas Christin and Reihaneh Safavi-Naini, editors, Financial Cryptography and Data Security, volume 8437 of Lecture Notes in Computer Science, pp. 119–135. Springer: Berlin, Germany, 2014.

43. Justine Sherry, Shaddi Hasan, Colin Scott, Arvind Krishnamurthy, Sylvia Ratnasamy, and Vyas Sekar. Making middleboxes someone else's problem: Network processing as a cloud service. In Proceedings of the ACM SIGCOMM 2012

Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pp. 13–24, 2012.

44. Zafar Ayyub Qazi, Cheng-Chun Tu, Luis Chiang, Rui Miao, Vyas Sekar, and Minlan Yu. Simplifying middlebox policy enforcement using SDN. In Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM, pp. 27–38, ACM: New York, 2013.

45. Aaron Gember, Robert Grandl, Junaid Khalid, and Aditya Akella. Design and implementation of a framework for so□ware-de□ned middlebox networking. In Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM, pp. 467–468, ACM: New York, 2013.

46. Je□rey R. Ballard, Ian Rae, and Aditya Akella. Extensible and scalable network monitoring using OpenSafe. In Proceedings of the 2010 Internet Network Management Conference on Research on Enterprise Networking, pp. 8–8, 2010.

47. Glen Gibb, Hongyi Zeng, and Nick McKeown. Outsourcing network functionality. In Proceedings of the First Workshop on Hot Topics in Software Defined Networks, pp. 73–78, ACM: New York, 2012.

48. Vyas Sekar, Ravishankar Krishnaswamy, Anupam Gupta, and Michael K. Reiter. Networkwide deployment of intrusion detection and prevention systems. In Proceedings of the 6th International Conference, Co-NEXT'10, pp. 18:1–18:12, ACM: New York, 2010.

49. Victor Heorhiadi, Michael K. Reiter, and Vyas Sekar. New opportunities for load balancing in network-wide intrusion detection systems. In Proceedings of the 8th International Conference on Emerging Networking Experiments and Technologies, CoNEXT'12, pp. 361–372, ACM: New York, 2012.

50. Saqib Raza, Guanyao Huang, Chen-Nee Chuah, Srini Seetharaman, and Jatinder Pal Singh. Measurouting: A framework for routing assisted tra□c monitoring. IEEE/ACM Transactions on Networking, 20(1):45–56, 2012.

51. Andreas Voellmy and Paul Hudak. Nettle: Taking the sting out of programming network routers. In Proceedings of the 13th International Conference on Practical Aspects of Declarative Languages, pp. 235–249, Springer-Verlag: Berlin, Germany, 2011.

52. Nate Foster, Michael J. Freedman, Rob Harrison,

Jennifer Rexford, Matthew L. Meola, and David Walker. Frenetic: A high-level language for OpenFlow networks. In Proceedings of the Workshop on Programmable Routers for Extensible Services of Tomorrow, pp. 6:1–6:6, ACM: New York, 2010.

53. Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. OpenFlow: Enabling innovation in campus networks. SIGCOMM Computer Communication Review, 38(2):69–74, 2008.

54. Philip Porras, Seungwon Shin, Vinod Yegneswaran, Martin Fong, Mabry Tyson, and Guofei Gu. A security enforcement kernel for OpenFlow networks. In Proceedings of the First Workshop on Hot Topics in Software Defined Networks, pp. 121–126, ACM: New York, 2012.

55. Seugwon Shin, Phillip Porras, Vinod Yegneswaran, Martin Fong, Guofei Gu, and Mabry Tyson. Fresco: Modular composable security services for so□ware-de□ned networks, 2013.

56. Seungwon Shin, Vinod Yegneswaran, Phillip Porras, and Guofei Gu. AVANT-GUARD: Scalable and vigilant switch □ow management in so□ware-de□ned networks. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, pp. 413– 424, ACM: New York, 2013.

57. L.R. Battula. Network Security Function Virtualization (NSFV) towards cloud computing with NFV over Open□ow infrastructure: Challenges and novel approaches. In ICACCI, 2014 International Conference on Advances in Computing, Communications and Informatics, pp. 1622–1628, 2014.

58. S. Shin, H. Wang, and G. Gu. A □rst step towards network security virtualization: From concept to prototype. IEEE Transactions on Information Forensics and Security, PP(99):1–1, 2015.

59. Seyed Kaveh Fayazbakhsh, Vyas Sekar, Minlan Yu, and Je□rey C. Mogul. FlowTags: Enforcing network-wide policies in the presence of dynamic middlebox actions. In Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, pp. 19–24, ACM: New York, 2013.

60. T. Ormandy. An empirical study into the security exposure to host of hostile virtualized environments. taviso.decsystem.org, 2007.

61. Joanna Rutkowska. Subverting vista kernel for fun and pro t. Black Hat Talk, 2006.

62. Tal Gar nkel, Keith Adams, Andrew War eld, and Jason Franklin. Compatibility is not transparency: VMM detection myths and realities. In Proceedings of the 11th USENIX Workshop on Hot Topics in Operating Systems, pp. 6:1-6:6, USENIX Association: Berkeley, CA, 2007.

63. Jason Franklin, Mark Luk, Jonathan M. McCune, Arvind Seshadri, Adrian Perrig, and Leendert van Doorn. Remote detection of virtual machine monitors with fuzzy benchmarking. SIGOPS Operating System Review, 42(3):83-92, 2008.

64. Flavio Lombardi and Roberto Di Pietro. Secure virtualization for cloud computing. Journal of Network and Computer Applications, 34(4):1113-1122, 2011.

65. Tal Gar nkel, Ben Pfa , Jim Chow, Mendel Rosenblum, and Dan Boneh. Terra: A virtual machine-based platform for trusted computing. In Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles, pp. 193-206, ACM: New York, 2003.

66. Stefan Berger, Ramón Cáceres, Kenneth A. Goldman, Ronald Perez, Reiner Sailer, and Leendert van Doorn. vTPM: Virtualizing the trusted platform module. In Proceedings of the 15th Conference on USENIX Security Symposium—Volume 15, USENIX Association, Berkeley, CA, 2006.

67. Brian Hay and Kara Nance. Forensics examination of volatile system data using virtual introspection. SIGOPS Operating System Review, 42(3):74-82, 2008.

68. Reiner Sailer, Trent Jaeger, Enriquillo Valdez, Ramon Caceres, Ronald Perez, Stefan Berger, John Linwood Gri n, and Leendert van Doorn. Building a MAC-based security architecture for the Xen open-source hypervisor. In Proceedings of the 21st Annual Computer Security Applications Conference, pp. 276-285, IEEE Computer Society: Washington, DC, 2005.

69. Ryan Riley, Xuxian Jiang, and Dongyan Xu. Guest-transparent prevention of kernel rootkits with VMM-based memory shadowing. In Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection, pp. 1-20, Springer-Verlag: Berlin, Germany, 2008.

70. Roberto Di Pietro, Flavio Lombardi, and Matteo Signorini. CloRExPa: Cloud resilience via execution path analysis. Future Generation Computer Systems, 32:168–179, 2014.

71. Z. Cli e Schreuders, Tanya McGill, and Christian Payne. Empowering end users to con ne their own applications: e results of a usability study comparing SELinux, AppArmor, and FBAC-LSM. ACM Transactions on Information and System Security, 14(2):19:1–19:28, 2011.

72. Hong Chen, Ninghui Li, and Ziqing Mao. Analyzing and comparing the protection quality of security enhanced operating systems. In NDSS. e Internet Society, 2009.

73. Robert N. M. Watson, Jonathan Anderson, Ben Laurie, and Kris Kennaway. Capsicum: Practical capabilities for UNIX. In Proceedings of the 19th USENIX Conference on Security, pp. 3–3, USENIX Association: Berkeley, CA, 2010.

74. Gansen Zhao, Chunming Rong, Jin Li, Feng Zhang, and Yong Tang. Trusted data sharing over untrusted cloud storage providers. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), pp. 97–103, 2010.

75. Masahiro Mambo and Eiji Okamoto. Proxy Cryptosystems: Delegation of the power to decrypt ciphertexts. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 80A(1):54–63, 1997.

76. Craig Gentry. Fully homomorphic encryption using ideal lattices. In Proceedings of the FortyFirst Annual ACM Symposium on Theory of Computing, pp. 169–178, ACM: New York, NY, 2009.

77. Craig Gentry. Computing arbitrary functions of encrypted data. Communications of the ACM, 53(3):97–105, 2010.

78. omas S. J. Schwarz and Ethan L. Miller. Store, forget, and check: Using algebraic signatures to check remotely administered storage. In Proceedings of the 26th IEEE International Conference on Distributed Computing Systems, pp. 12–, IEEE Computer Society: Washington, DC, 2006.

79. Mark Lillibridge, Sameh Elnikety, Andrew Birrell, Mike Burrows, and Michael Isard. A cooperative internet backup scheme. In Proceedings of the Annual Conference on USENIX

Annual Technical Conference, pp. 3–3, USENIX Association: Berkeley, CA, 2003.

80. Kevin D. Bowers, Ari Juels, and Alina Oprea. Hail: A high-availability and integrity layer for cloud storage. In Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 187–198, ACM: New York, 2009.

81. Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou. Ensuring data storage security in cloud computing. In 17th International Workshop on Quality of Service, 2009, pp. 1–9, 2009.

82. Danny Harnik, Benny Pinkas, and Alexandra Shulman-Peleg. Side channels in cloud services: Deduplication in cloud storage. IEEE Security and Privacy, 8(6):40–47, 2010.

83. Andrew C. Myers and Barbara Liskov. Protecting privacy using the decentralized label model. ACM Transactions on Software Engineering and Methodology, 9(4):410–442, 2000.

84. Ioannis Papagiannis, Matteo Migliavacca, David M. Eyers, Brian Shand, Jean Bacon, and Peter Pietzuch. Enforcing user privacy in web applications using erlang. Web 2.0 Security and Privacy, 2010.

85. Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, Advances in Cryptology—CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pp. 213–229. Springer: Berlin, Germany, 2001.

86. Lishan Kang and Xuejie Zhang. Identity-based authentication in cloud storage sharing. In 2010 International Conference on Multimedia Information Networking and Security, pp. 851–855, 2010.

87. Qin Liu, Guojun Wang, and Jie Wu. Eﬀcient sharing of secure cloud storage services. In 2010 IEEE 10th International Conference on Computer and Information Technology, pp. 922–929, 2010.

88. Craig Gentry and Alice Silverberg. Hierarchical id-based cryptography. In Yuliang Zheng, editor, Advances in Cryptology—ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, pp. 548–566, Springer: Berlin, Germany, 2002.

89. Jin Li, Gansen Zhao, Xiaofeng Chen, Dongqing Xie,

Chunming Rong, Wenjun Li, Lianzhang Tang, and Yong Tang. Fine-grained data access control systems with user accountability in cloud computing. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), pp. 89–96, 2010.

90. Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques, pp. 457–473, Springer-Verlag: Berlin, Germany, 2005.

91. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for ne-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89–98, ACM: New York, 2006.

92. Melissa Chase and Sherman S.M. Chow. Improving privacy and security in multi-authority attribute-based encryption. In Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 121–130, ACM: New York, 2009.

93. Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable, and negrained data access control in cloud computing. In Proceedings of the 29th Conference on Information Communications, pp. 534–542, IEEE Press: Piscataway, NJ, 2010.

94. Seny Kamara and Kristin Lauter. Cryptographic cloud storage. In Proceedings of the 14th International Conference on Financial Cryptography and Data Security, pp. 136–149, SpringerVerlag, Berlin, Germany, 2010.

14 Chapter 14: Designing Cloud Security and Operations Models in the Changed Geopolitical Environment

1. Sajee Mathew. Overview of Amazon Web Services. Whitepaper. Amazon Web Services: Seattle, WA. November 2014. https://d0.awsstatic.com/whitepapers/aws-overview.pdf.

2. Gethyn Ellis. Microsoft Azure IaaS Essentials. Packt Publishing. May 2015.

3. Tom Fi□eld, Diane Felming, Anne Gentle, Lorin Hochstein, Jonathan Proulx, Everett Toews, Joe Topjian. OpenStack Operations Guide—Setup and Manage Your Openstack Cloud. O'Reilly Media. September 2015. http://docs.openstack.org/ops/. Web proxies Load balancer Customer Corporate Network Internet Cloud provider SSH jumphost Windows terminal Administration tools Customer cloud servers VPC VPN gateway

FIGURE 14.10 Example private cloud architecture.

4. The ABCs of Continuous Release and Deploy in a DevOps Approach. Technical White Paper. IBM: Somers, NY. May 2013.

5. Amazon Elastic Compute Cloud: User Guide, Regions and Availability Zones. Amazon Web Services: Seattle, WA. April 2015. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html.

6. Assurance Reports on Controls at a Service Organization (ISAE 3402). International Auditing and Assurance Standards Board. June 2011. http://isae3402.com.

7. Statement on Standards for Attestation Engagements No. 16 (SSAE 16). Auditing Standards Board of the American Institute of Certi□ed Public Accountants (AICPA). April 2010. http://ssae16.com.

8. ISO/IEC 27001—Information Security Management Standard. International Organization for Standardization (ISO): Vernier, Switzerland. 2013. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

9. SA Security, Trust & Assurance Registry (STAR). Cloud Security Alliance Group: Seattle, WA. 2015.

https://cloudsecurityalliance.org/star/#_overview.

10. On Amendments to Certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunications Networks. Russian Federal Law No. 242-FZ. July 2014. http://www.rg.ru/2014/07/23/persdannye-dok.html.

11. Register of Operators Engaged in the Processing of Personal Data. Government of the Russian Federation. Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor). September 2015. http://rkn.gov.ru/personal-data/register/.

12. Steve Dickinson. Foreign SaaS in China: Get off of my Cloud. China Law Blog. Harris & Moure: Seattle, WA. April 2015.

13. European Parliament and Commission. 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. July 2000. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

14. Payment Card Industry (PCI) Data Security Standard—Requirements and Security Assessment Procedures. Version 3.1. PCI Security Standards Council: Wake□eld, MA. April 2015. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf.

15. Martijn Jansen. Troopers Security Conference: How to Work Towards Pharma Compliance for Cloud Computing. ERNW Enno Rey Netzwerke GmbH: Heidelberg, Germany. 2014. https://www.

16. Security and Privacy Controls for Federal Information Systems and Organizations. Revision 4. National Institute of Standards and Technology. January 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

17. Security Requirements for Cryptographic Modules. Federal Information Processing Standard. FIPS PUB 140-2. May 2001. http://csrc.nist.gov/publications/□ps/□ps140-2/□ps1402.pdf.

18. Isabel Münch, Michael Hange. IT-Grundschutz-Catalogues.

13th version. German Federal O ce for Information Security (BSI). 2013. https://gsb.download.bva.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf.

19. Dr Paul Taloni. Information Security Manual—Controls 2015. Version 2015. Australian Signals Directorate: Kingston ACT, Australia. 2015. http://www.asd.gov.au/publications/Information_Security_Manual_2015_Controls.pdf.

20. Amazon Virtual Private Cloud: Getting Started Guide. Amazon Web Services: Seattle, WA. April 2015.

15 Chapter 15: Continuous Private Cloud Security Monitoring

1. Joshua Brower. SANS Institute Whitepaper. The Security Onion Cloud Client—Network Security Monitoring for the Cloud. 2013. http://www.sans.org/reading-room/whitepapers/

2. Gethyn Ellis. Managing and Monitoring Virtual Machines. Chapter 5 in Microsoft Azure IaaS Essentials. Packt Publishing Ltd. 2015.

3. Amazon CloudWatch: Developer Guide. Amazon Web Services: Seattle, WA. 2015. http://docs.

4. Intelligent Monitoring for your AWS Infrastructure, Systems and App. Stackdriver: Boston, MA. 2015. http://www.stackdriver.com/event-logging/.

5. AWS CloudTrail: User Guide. Version 1.0. Amazon Web Services: Seattle, WA. 2015. http://

6. Assurance Reports on Controls at a Service Organization (ISAE 3402). International Auditing and Assurance Standards Board. 2011. http://isae3402.com.

7. Statement on Standards for Attestation Engagements No. 16 (SSAE 16). Auditing Standards Board of the American Institute of Certiﬁed Public Accountants (AICPA). April 2010. http:// ssae16.com.

8. ISO/IEC 27001—Information Security Management Standard. International Organization for Standardization (ISO): Geneva, Switzerland. 2013.

9. SA Security, Trust & Assurance Registry (STAR). Cloud Security Alliance Group. Seattle, WA. 2015. https://cloudsecurityalliance.org/star/#_overview.

16 Chapter 16: Cloud Security Assessment and Authorization

1. Joint Task Force Transformation Initiative. NIST Special Publication 800-37 Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010.

2. Joint Task Force Transformation Initiative. NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

3. FedRAMP. Guide to Understanding FedRAMP. Version 2.0, June 2014.

4. VanRoekel, Steven. Security Authorization of Information Systems in Cloud Computing Environments. O ce of Management and Budget (OMB) Memorandum, December 8, 2011.

5. FedRAMP. FedRAMP Security Assessment Framework. Version 2.0, June 2014.

17 Chapter 17: Assessment and Authorization in Private Cloud Security

1. Claudio A. Ardagna, Rasool Asal, Ernesto Damiani, and Quang Hieu Vu. From security to assurance in the cloud: A survey. ACM Computing Surveys, 48(1):2:1–2:50, July 2015.

2. Wylve and Bikeborg. Cloud Computing Layers. Wikimedia Foundation: San Francisco, CA. 2010.

3. European Union Agency for Network and Information Security (ENISA). Cloud Computing Risk Assessment. ENISA: Heraklion, Greece. http://www.enisa.europa.eu/activities/risk-management/

4. Cloud Security Alliance. Seattle, WA. https://cloudsecurityalliance.org/star.

5. P. Saripalli and B. Walters. QUIRC: A quantitative impact and risk assessment framework for cloud security. In IEEE 3rd International Conference on Cloud Computing, pp. 280–288, July 2010.

6. Burton S. Kaliski, Jr. and Wayne Pauley. Toward risk assessment as a service in cloud environments. In Proceedings of the 2Nd USENIX Conference on Hot Topics in Cloud Computing, pp. 13–13, USENIX Association: Berkeley, CA, 2010.

7. Je□rey O. Kephart and David M. Chess. □e vision of autonomic computing. Computer, 36(1):41–50, January 2003.

8. Ari Juels and Burton S. Kaliski, Jr. Pors: Proofs of retrievability for large □les. In Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 584–597, ACM: New York, 2007.

9. Christian Cachin, Idit Keidar, and Alexander Shraer. Trusting the cloud. SIGACT News, 40(2):81–86, June 2009.

10. E. Zahoor, O. Perrin, and A. Bouchami. Catt: A cloud based authorization framework with trust and temporal aspects. In 2014 International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), pp. 285–294, October 2014.

11. Christian Mainka, Vladislav Mladenov, Florian Feldmann, Julian Krautwald, and Jo¨rg Schwenk. Your so□ware at my service: Security analysis of saas single sign-on solutions in the cloud. In Proceedings of the 6th Edition of the ACM

Workshop on Cloud Computing Security, pp. 93–104, ACM: New York, 2014.

12. Rahat Masood, MuhammadAwais Shibli, Yumna Ghazi, Ayesha Kanwal, and Arshad Ali. Cloud authorization: Exploring techniques and approach towards e□ective access control framework. Frontiers of Computer Science, 9(2):297–321, 2015.

13. Durgesh Bajpai, Manu Vardhan, Sachin Gupta, Ravinder Kumar, and DharmenderSingh Kushwaha. Security service level agreements based authentication and authorization model for accessing cloud services. In Natarajan Meghanathan, Dhinaharan Nagamalai, and Nabendu Chaki, editors, Advances in Computing and Information Technology, volume 176 of Advances in Intelligent Systems and Computing, pp. 719–728, Springer: Berlin, Germany, 2012.

14. FuzzyBSc. Role Based Access Control. Wikimedia Foundation: San Francisco, CA, 2013. https://upload.wikimedia.org/wikipedia/en/c/c3/RBAC.jpg.

15. Salim Khamadja, Kamel Adi, and Luigi Logrippo. Designing □exible access control models for the cloud. In Proceedings of the 6th International Conference on Security of Information and Networks, pp. 225–232, ACM: New York, 2013.

16. Shi-Xin Luo, Feng-Mei Liu, and Chuan-Lun Ren. A hierarchy attribute-based access control model for cloud storage. In International Conference on Machine Learning and Cybernetics, vol. 3, pp. 1146–1150, July 2011.

17. Syed Rizvi, Jungwoo Ryoo, John Kissell, and Bill Aiken. A stakeholder-oriented assessment index for cloud security auditing. In Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication, pp. 55:1–55:7, ACM: New York, 2015.

18. Oleg Makarevich, Irina Mashkina, and Alina Sentsova. □e method of the information security risk assessment in cloud computing systems. In Proceedings of the 6th International Conference on Security of Information and Networks, pp. 446–447, ACM: New York, 2013.

19. Marjan Gusev, Sasko Ristov, and Aleksandar Donevski. Security vulnerabilities from inside and outside the eucalyptus cloud. In Proceedings of the 6th Balkan Conference in Informatics, pp. 95–101, ACM: New York, 2013.

20. A. Donevski, S. Ristov, and M. Gusev. Security assessment of virtual machines in open source clouds. In 36th International Convention on Information Communication Technology Electronics Microelectronics (MIPRO), pp. 1094–1099, May 2013.

21. David W. Chadwick and Kaniz Fatema. A privacy preserving authorisation system for the cloud. Journal of Computer and System Sciences, 78(5):1359–1373, 2012.

22. Younis A. Younis, Kashif Kifayat, and Madjid Merabti. An access control model for cloud computing. Journal of Information Security and Applications, 19(1):45–60, 2014.

23. Fernandes et al. 2013.

24. Gruschka and Jensen. 2010.

25. Nils Gruschka and Luigi Lo Iacono. Vulnerable cloud: Soap message security validation revisited. In IEEE International Conference on Web Services, 2009, pp. 625–631, IEEE, 2009.

26. McIntosh and Austel. 2005.

27. Meiko Jensen, Jo¨rg Schwenk, Nils Gruschka, and Luigi Lo Iacono. On technical security issues in cloud computing. In IEEE International Conference onCloud Computing, pp. 109–116, IEEE, 2009.

28. Juraj Somorovsky, Mario Heiderich, Meiko Jensen, Jo¨rg Schwenk, Nils Gruschka, and Luigi Lo Iacono. All your clouds are belong to us: Security analysis of cloud management interfaces. In Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, pp. 3–14, ACM: New York, 2011.

29. Ashley Chonka, Yang Xiang, Wanlei Zhou, and Alessio Bonti. Cloud security defence to protect cloud computing against http-dos and xml-dos attacks. Journal of Network and Computer Applications, 34(4):1097–1107, 2011.

30. Mudhakar Srivatsa, Ling Liu, and Arun Iyengar. Eventguard: A system architecture for securing publish-subscribe networks. ACM Transactions on Computer Systems (TOCS), 29(4):10, 2011.

31. Bugiel et al. 2011.

32. Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 199–212, ACM: New York, 2009.

33. Amittai Aviram, Sen Hu, Bryan Ford, and Ramakrishna Gummadi. Determinating timing channels in compute clouds. In Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, pp. 103–108, ACM: New York, 2010.

34. Michael Pearce, Sherali Zeadally, and Ray Hunt. Virtualization: Issues, security threats, and solutions. ACM Computing Surveys, 45(2):17:1–17:39, March 2013.

18 Chapter 18: Advanced Security Architectures for Private Cloud Computing

1. Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing V3.0, 2011.

2. Mike Edwards. Cloud computing ISO security and privacy standards: 27017, 27018, 27001, 2015.

3. Vaibhav Khadilkar, Anuj Gupta, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham. Secure data storage and retrieval in the cloud. University of Texas, 2011.

4. S. Srinivasan. Is security realistic in cloud computing?. Journal of International Technology and Information Management, 22(4), Article 3, 2014.

5. Google. Google Cloud Platform. Google.com. Retrieved November 25, 2014. 192.168.1.35/27192.168.1.62/27 VPN point to point Domain controller 192.168.1.61/27 192.168.1.1/27 192.168.1.2/27 Border router/modem and NAT Firewall 192.168.1.65/27 192.168.1.98/27 1 9 2 . 1 6 8 . 1 . 3 3 / 2 7 1 9 2 . 1 6 8 . 1 . 9 7 / 2 7 192.168.1.60/27 192.168.1.34/27 192.168.1.35/27 ATM Layer 3 switch Layer 3 switch Layer 2 switch Layer 2 switch Security cameras (×4) LA employee computers (×20) Layer 2 switch Layer 2 switch Layer 3 switch WiFi AP ATM (×2) Database server IP2 IP1 IP3 IP4 Internet Public IP-ISP provided ISP (Time Warner) MRT Credit Union-logical network diagram – phase III 192.168.1.66/27192.168.1.94/27 LA main office 192.168.1.99/27192.168.1.126/27 On-site data center 1 9 2 . 1 6 8 . 1 . 6 4 / 2 7

FIGURE 18.7 LA IT data center.

19 Chapter 19: Advanced Private Cloud Computing Security Architectures

1. VCE Company, LLC. Enabling Trusted Multi-Tenancy with Vblock ® Systems. VCE Company, LLC: Richardson, TX, pp. 8–42, 2015.

2. Peter Mell and Timothy Grance. The NIST Definition of Cloud Computing. ̄e National Institute of Standards and Technology: Gaithersburg, MD, pp. 5–7, 2011. http://csrc.nist.gov/ publications/nistpubs/800-145/SP800-145.pdf.

3. Bill Loe̱er and Jim Dial. Private Cloud Principles, Concepts, and Patterns. Microso̱ TechNet Article, Microso̱ Corp., 2013. http://social.technet.microso̱.com/wiki/contents/

4. Dob Todorov and Yinal Ozkan. AWS Security Best Practices. Amazon Web Services, pp. 1–52, 2013.

5. Cisco Corporation. Architecture Overview for FlexPod with Microsoft Windows Server 2008 R2 and Microsoft System Center 2012. pp. 45–83, 2012. http://www.cisco.com/c/dam/en/us/

6. Bill Loe̱er and Jim Dial. Private Cloud Security Operations Principles. Microso̱ TechNet Article, Microso̱ Corp., 2013. http://social.technet.microso̱.com/wiki/contents/articles/ 6658. private-cloud-security-operations-principles.aspx.

7. Brian Lowans, Neil MacDonald, and Carsten Casper. Five Cloud Data Residency Issues That Must Not Be Ignored. Gartner: Stamford, CT, pp. 13–25, 2012. https://www.gartner.com/ doc/2288615.

8. Intel ® Cloud Builders Guide. Integrating Intel® TXT Enabled Clouds with McAfee Security Management Platform Leveraging Trapezoid Trust Control Suite, pp. 6–12, 2013. http://trapezoid . com/images/pdf/Intel_Cloud_Builders_Trapezoid_McAfee.pdf.

9. Intel ® Cloud Builders Guide. Integrating Intel® IPT with OPT and Symantec∗ VIP for Dynamically Assigning Permissions to Cloud Resources, pp. 4–21, 2013. http://trapezoid.com/ images/pdf/Intel_Cloud_Builders_Intel_IPT_2013.pdf.

20 Chapter 20: Privacy Protection in Cloud Computing through Architectural Design

1. ibodeau, P. Snowden revelations may cost U.S. cloud providers billions, says study. http://

2. Gentry, C. A fully homomorphic encryption scheme. PhD thesis, Stanford University, Stanford, CA. crypto.stanford.edu/craig (2009).

3. Chen, Y.Y., Jamkhedkar, P.A., Lee, R.B. A so ware-hardware architecture for self- protecting data. In 19th ACM Conference on Computer and Communications Security. Raleigh, NC (October 16–18, 2012).

4. Lie, D., ekkath, C., Mitchell, M., Lincoln, P., Boneh, D., Mitchell, J., Horowitz, M. Architectural support for copy and tamper resistant so ware. SIGPLAN Not. 35(11) (November 2000): 168–177.

5. Chen, X., Gar nkel, T., Lewis, E.C., Subrahmanyam, P., Waldspurger, C.A., Boneh, D., Dwoskin, J., Ports, D.R. Overshadow: A virtualization-based approach to retro tting protection in commodity operating systems. In ASPLOS XIII: Proceedings of the 13th International Conference on Architectural Support for Programming Languages and Operating Systems. ACM: New York (2008) 2–13.

6. Butt, S., Lagar-Cavilla, H.A., Srivastava, A., Ganapathy, V. Self-service cloud computing. In Proceedings of the 2012 ACM Conference on Computer and Communications Security. ACM: New York (2012) 253–264.

7. Li, M., Zang, W., Bai, K., Yu, M., Liu, P. Mycloud—Supporting user-con gured privacy protection in cloud computing. In Annual Computer Security Applications Conference. New Orleans, LA (December 2013).

8. Pan, W., Zhang, Y., Yu, M., Jing, J. Improving virtualization security by splitting hypervisor into smaller components. In Cuppens-Boulahia, N., Cuppens, F., Garcia-Alfaro, J., eds. Data and Applications Security and Privacy XXVI. Volume 7371 of Lecture Notes in Computer Science. Springer: Berlin, Germany (2012) 298–313.

9. Murray, D., Milos, G., Hand, S. Improving xen security through disaggregation. In Proceedings of the Fourth ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments. ACM: New York (2008) 151–160.

10. Zhang, F., Chen, J., Chen, H., Zang, B. Cloudvisor: Retroﬁtting protection of virtual machines in multi-tenant cloud with nested virtualization. In Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles. ACM: New York (2011) 203–216.

11. Williams, D., Jamjoom, H., Weatherspoon, H. The Xen-Blanket: Virtualize Once, Run Everywhere. ACM EuroSys (2012).

12. Ben-Yehuda, M., Day, M., Dubitzky, Z., Factor, M., Har'El, N., Gordon, A., Liguori, A., Wasserman, O., Yassour, B. ﬁe turtles project: Design and implementation of nested virtualization. In Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation. USENIX Association (2010) 1–6.

13. Kauer, B., Verissimo, P., Bessani, A. Recursive virtual machines for advanced security mechanisms. In IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops. IEEE (2011) 117–122.

14. Chuang, I.H., Li, S.H., Huang, K.C., Kuo, Y.H. An eﬀective privacy protection scheme for cloud computing. In 13th International Conference on Advanced Communication Technology (February 2011) 260–265.

15. Steinberg, U., Kauer, B. Nova: A microhypervisor-based secure virtualization architecture. In Proceedings of the 5th European Conference on Computer Systems. ACM: New York (2010) 209–222.

16. Heiser, G., Uhlig, V., LeVasseur, J. Are virtual-machine monitors microkernels done right? SIGOPS Oper. Syst. Rev. 40(1) (January 2006) 95–99.

17. Klein, G., Elphinstone, K., Heiser, G., Andronick, J., Cock, D., Derrin, P., Elkaduwe, D., Engelhardt, K., Kolanski, R., Norrish, M., Sewell, T., Tuch, H., Winwood, S. seL4: Formal veriﬁcation of an OS kernel. In Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles. ACM: New York (2009) 207–220.

18. Nguyen, A., Schear, N., Jung, H., Godiyal, A., King, S., Nguyen, H. MAVMM: Lightweight and purpose built VMM for malware analysis. In Annual Computer Security Applications Conference, 2009. IEEE (2009) 441–450.

19. McCune, J., Li, Y., Qu, N., Zhou, Z., Datta, A.,

Gligor, V., Perrig, A. TrustVisor: Eﬀcient TCB reduction and attestation. In 2010 IEEE Symposium on Security and Privacy (SP). IEEE (2010) 143–158.

20. Intel Inc. Intel® 64 and IA-32 Architectures Software Developer Manuals (2009).

21. Intel Coperation. Intel® Trusted Execution Technology (2011).

22. Azab, A., Ning, P., Zhang, X. SICE: A hardware-level strongly isolated computing environment for ×86 multi-core platforms. In Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM: New York (2011) 375–388.

23. McCune, J.M., Parno, B.J., Perrig, A., Reiter, M.K., Isozaki, H. Flicker: An execution infrastructure for TCB minimization. SIGOPS Oper. Syst. Rev. 42(4) (April 2008) 315–328.

24. Keller, E., Szefer, J., Rexford, J., Lee, R. NoHype: Virtualized cloud infrastructure without the virtualization. In ACM SIGARCH Computer Architecture News. Vol. 38. ACM: New York (2010) 350–361.

25. Szefer, J., Keller, E., Lee, R., Rexford, J. Eliminating the hypervisor attack surface for a more secure cloud. In Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM: New York (2011) 401–412.

26. Biederman, E. Kernel korner: About LinuxBIOS. Linux J. 2001(92) (December 2001) 7–.

27. Bleikertz, S., Kurmus, A., Nagy, Z.A., Schunter, M. Secure cloud maintenance: Protecting workloads against insider attacks. In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM: New York (2012) 83–84.

28. Song, D., Shi, E., Fischer, I., Shankar, U. Cloud data protection for the masses. Computer 45(1) (2012) 39–45.

29. Popek, G.J., Goldberg, R.P. Formal requirements for virtualizable third generation architectures. Commun. ACM 17(7) (July 1974) 412–421.

30. Belpaire, G., Hsu, N.T. Formal properties of recursive virtual machine architectures. In Proceedings of the Fifth

ACM Symposium on Operating Systems Principles. ACM: New York (1975) 89–96.

31. Belpaire, G., Hsu, N.T. Formal properties of recursive virtual machine architectures. SIGOPS Oper. Syst. Rev. 9(5) (November 1975) 89–96.

32. Wang, Z., Lee, R.B. New cache designs for thwarting so□ware cache-based side channel attacks. In Proceedings of the 34th Annual International Symposium on Computer Architecture. ACM: New York (2007) 494–505.

33. Halfond, W.G.J., Orso, A., Manolios, P. Using positive tainting and syntax-aware evaluation to counter SQL injection attacks. In SIGSOFT '06/FSE-14: Proceedings of the 14th ACM SIGSOFT International Symposium on Foundations of Software Engineering. ACM: New York (2006) 175–185.

34. Haldar, V., Chandra, D., Franz, M. Dynamic taint propagation for java. In 21st Annual Computer Security Applications Conference (December 5–9, 2005) 9pp.

35. Luk, C.K., Cohn, R.S., Muth, R., Patil, H., Klauser, A., Lowney, P.G., Wallace, S., Reddi, V.J., Hazelwood, K.M. Pin: Building customized program analysis tools with dynamic instrumentation. In PLDI (2005) 190–200.

36. Pfoh, J., Schneider, C., Eckert, C. A formal model for virtual machine introspection. In: VMSec '09: Proceedings of the 1st ACM Workshop on Virtual Machine Security. ACM: New York (2009) 1–10.

37. Anderson, R., Kuhn, M. Tamper resistance—A cautionary note. In Proceedings of the Second Usenix Workshop on Electronic Commerce. Volume 2. (1996) 1–11.

38. Anderson, R., Kuhn, M. Tamper resistance: A cautionary note. In Proceedings of the 2nd Conference on Proceedings of the Second USENIX Workshop on Electronic Commerce. Volume 2. USENIX Association: Berkeley, CA (1996) 1–1.

39. Wojtczuk, R., Rutkowska, J. Attacking SMM memory via Intel CPU cache poisoning. In Invisible Things Lab (2009).

40. Tomlinson, A. Introduction to the TPM. In Smart Cards, Tokens, Security and Applications (2008) 155–172.

41. Gar□nkel, T., Pfa□, B., Chow, J., Rosenblum, M., Boneh, D. Terra: A virtual machine-based platform for trusted

computing. In ACM SIGOPS Operating Systems Review. Volume 37. ACM: New York (2003) 193–206.

42. Singaravelu, L., Pu, C., Härtig, H., Helmuth, C. Reducing TCB complexity for security- sensitive applications: Three case studies. SIGOPS Oper. Syst. Rev. 40(4) (April 2006) 161–174.

43. Klein, G., Elphinstone, K., Heiser, G., Andronick, J., Cock, D., Derrin, P., Elkaduwe, D., Engelhardt, K., Kolanski, R., Norrish, M., Sewell, T., Tuch, H., Winwood, S. seL4: Formal verification of an OS kernel. In Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles. ACM: New York (2009) 207–220.

44. Jhala, R., Majumdar, R. Software model checking. ACM Comput. Surv. 41(4) (October 2009) 21:1–21:54.

45. Advanced Micro Devices. AMD64 Architecture Programmer's Manual Volume 2: System Programming (December 2011).

46. Intel Corporation. Intel® Virtualization Technology Specification for Directed I/O Specification. www.intel.com/technology/vt/.

47. Advanced Micro Devices. AMD I/O Virtualization Technology (IOMMU) Specification (February 2009).

48. Intel Corporation. Intel® PCI-SIG SR-IOV Primer: An Introduction to SR-IOV Technology (January 2011).

49. Meth, K.Z., Satran, J. Design of the iSCSI protocol. In Proceedings of the 20th IEEE/11th NASA Goddard Conference on Mass Storage Systems and Technologies. IEEE Computer Society: Washington, DC (2003) 116–.