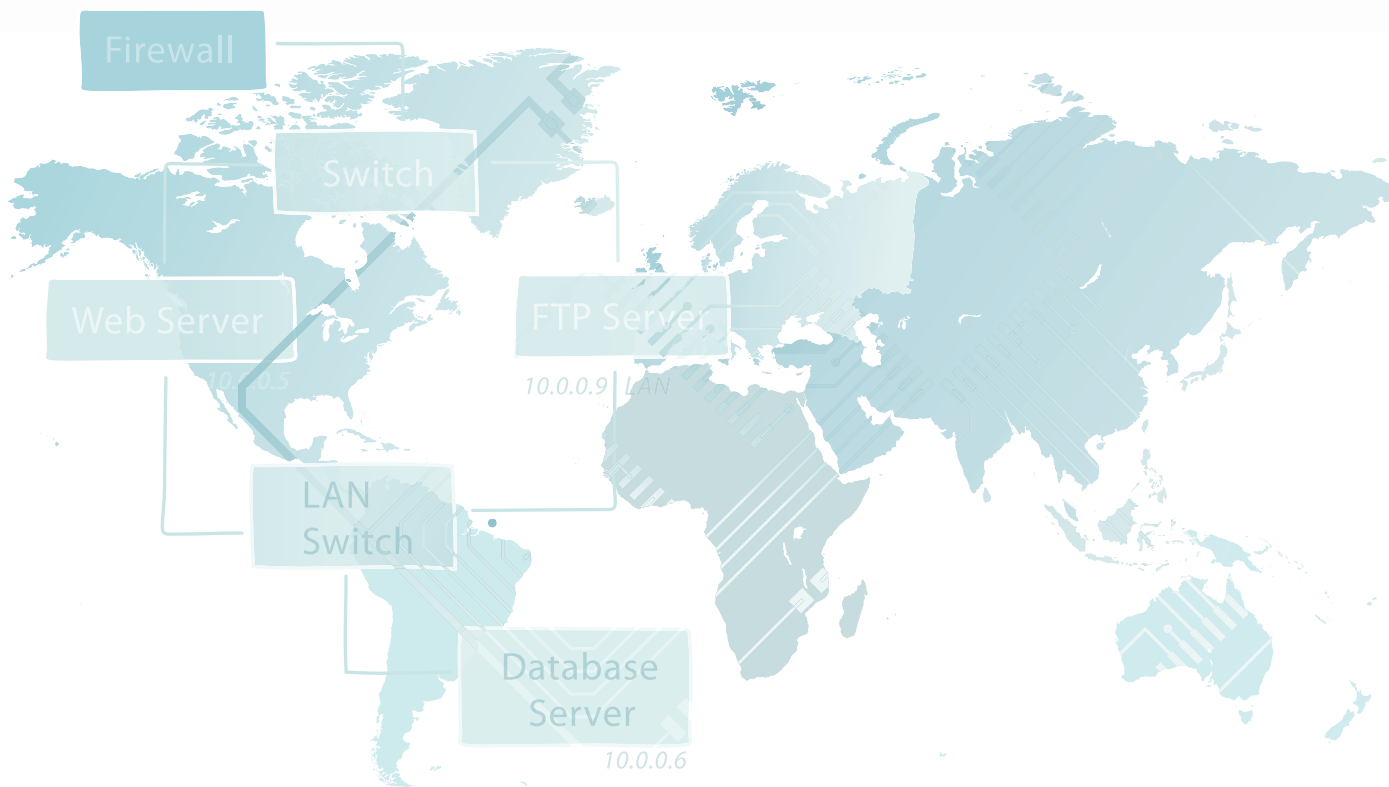


CLOUD SECURITY

A Comprehensive Guide to Secure Cloud Computing



Ronald L. Krutz and Russell Dean Vines



Contents at a Glance

Foreword		xxi
Introduction		xxiii
Chapter 1	Cloud Computing Fundamentals	1
Chapter 2	Cloud Computing Architecture	33
Chapter 3	Cloud Computing Software Security Fundamentals	61
Chapter 4	Cloud Computing Risk Issues	125
Chapter 5	Cloud Computing Security Challenges	153
Chapter 6	Cloud Computing Security Architecture	177
Chapter 7	Cloud Computing Life Cycle Issues	217
Chapter 8	Useful Next Steps and Approaches	259
Glossary of Terms and Acronyms		279
References		345
Index		349

Cloud Security



Cloud Security

A Comprehensive Guide to Secure Cloud Computing

Ronald L. Krutz
Russell Dean Vines



WILEY

Wiley Publishing, Inc.

Cloud Security: A Comprehensive Guide to Secure Cloud Computing

Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Copyright © 2010 by Wiley Publishing, Inc., Indianapolis, Indiana
Published simultaneously in Canada

ISBN: 978-0-470-58987-8

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Control Number: 2010930374

Trademarks: Wiley, the Wiley logo, Wrox, the Wrox logo, Programmer to Programmer, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

I thank God for His greatest gift of all—my family.

— Ronald L. Krutz

Dedicated to Elzy, for now and forever.

— Russell Dean Vines

About the Authors



Ronald L. Krutz is a senior information system security consultant. He has over 30 years of experience in distributed computing systems, computer architectures, real-time systems, information assurance methodologies, and information security training. He holds B.S., M.S., and Ph.D. degrees in Electrical and Computer Engineering and is the author of best selling texts in the area of information system security.

He co-authored the *CISSP Prep Guide* for John Wiley and Sons and is co-author of the *Wiley Advanced CISSP Prep Guide*, the *CISSP Prep Guide, Gold Edition*, the *Security+ Certification Guide*, the *CISM Prep Guide*, the *CISSP Prep Guide, 2nd Edition: Mastering CISSP and ISSEP*, the *Network Security Bible*, the *CISSP and CAP Prep Guide, Platinum Edition: Mastering CISSP and CAP*, the *Certified Ethical Hacker (CEH) Prep Guide*, and the *Certified Secure Software Lifecycle Prep Guide*. He is also the author of *Securing SCADA Systems* and of three textbooks in the areas of microcomputer system design, computer interfacing, and computer architecture. Dr. Krutz has seven patents in the area of digital systems and has published over 40 technical papers.

Dr. Krutz also serves as consulting Editor for John Wiley and Sons Information Security Certification Series, is a Distinguished Visiting Lecturer in the University of New Haven Henry C. Lee College of Criminal Justice and Forensic Sciences, and is an Adjunct Professor in Midway College, Kentucky.

Dr. Krutz is a Registered Professional Engineer in Pennsylvania.



Russell Dean Vines has been in the information systems industry for over 20 years, and has a unique ability to disseminate complex security issues to a wider audience, from CEOs to home Internet surfers.

He is also the author or co-author of 10 previous books, including the *CISSP Prep Guide*, which reached #25 on Amazon's best-sellers list. He co-authored the *Advanced CISSP Prep Guide*, the *CISSP Prep Guide, Gold Edition*, the *Security+ Certification Guide*, the *CISM Prep Guide*, the *CISSP Prep Guide, 2nd Edition: Mastering CISSP and ISSEP*, the *CISSP and CAP Prep Guide, Platinum Edition: Mastering CISSP and CAP*, and the *Certified Ethical Hacker (CEH) Prep Guide*. He is also the author of *Wireless Security Essentials*, and *Composing Digital Music for Dummies*.

In addition to being a Certified Information Systems Security Professional (CISSP), Mr. Vines is a Certified Information Systems Manager (CISM), a Certified Ethical Hacker (CEH), certified in CompTIA's Security+ program, and is a Payment Card Industry (PCI) Qualified Security Assessor (QSA). Russ also has vendor security certifications from RSA, Websense, McAfee, Citrix, VMware, Microsoft, and Novell, and has been trained in the NSA's Information Assurance Methodology (IAM).

Mr. Vines is a frequent contributor to Web and trade publications; discusses Information Security Threats and Countermeasures as a member of SearchSecurityChannel.com's Ask the Experts panel, frequently speaks at industry events such as Comdex and Network+Interop, and teaches CISSP, CEH, and Websense classes.



Executive Editor

Carol Long

Project Editor

Ed Connor

Technical Editor

David Chapa

Production Editor

Daniel Scribner

Editorial Director

Robyn B. Siesky

Editorial Manager

Mary Beth Wakefield

Marketing Manager

David Mayhew

Production Manager

Tim Tate

**Vice President and Executive
Group Publisher**

Richard Swadley

**Vice President and Executive
Publisher**

Barry Pruett

Associate Publisher

Jim Minatel

**Project Coordinator,
Cover**

Lynsey Stanford

Proofreader

Nancy Bell

Indexer

Robert Swanson

Cover Designer

Ryan Sneed

Cover Image

© istockphoto.com/
GodfriedEdelman



Acknowledgments

I want to thank my wife, Hilda, for her support and encouragement during the writing of this text.

— Ronald L. Krutz

I'd like to give a big shout-out to the gang at Gotham Technology Group, in particular Ken Phelan, Joe Jessen, and Nancy Rand, for their assistance during this project. I'd also like to thank doctors Paul M. Pellicci and Lawrence Levin for the rare gift of health. But my greatest thanks is reserved for my wife, Elzy, for her continuous and unwavering support throughout my life.

— Russell Dean Vines

Both authors would like to express their gratitude to Carol Long and Ed Connor of John Wiley and Sons for their support and assistance in developing this text.



Contents

Foreword		xxi
Introduction		xxiii
Chapter 1	Cloud Computing Fundamentals	1
	What Cloud Computing Isn't	7
	Alternative Views	8
	Essential Characteristics	9
	On-Demand Self-Service	9
	BroadNetwork Access	10
	Location-Independent Resource Pooling	10
	Rapid Elasticity	10
	Measured Service	11
	Architectural Influences	11
	High-Performance Computing	11
	Utility and Enterprise Grid Computing	14
	Autonomic Computing	15
	Service Consolidation	16
	Horizontal Scaling	16
	Web Services	17
	High-Scalability Architecture	18
	Technological Influences	18
	Universal Connectivity	18
	Commoditization	19
	Excess Capacity	20
	Open-Source Software	21
	Virtualization	22
	Operational Influences	23
	Consolidation	23

	Outsourcing	26
	Outsourcing Legal Issues	26
	Business Process Outsourcing (BPO) Issues	28
	IT Service Management	30
	Automation	31
	Summary	31
Chapter 2	Cloud Computing Architecture	33
	Cloud Delivery Models	34
	The SPI Framework	34
	SPI Evolution	34
	The SPI Framework vs. the Traditional IT Model	35
	Cloud Software as a Service (SaaS)	37
	Benefits of the SaaS Model	38
	Cloud Platform as a Service (PaaS)	39
	Cloud Infrastructure as a Service (IaaS)	41
	Cloud Deployment Models	43
	Public Clouds	44
	Community Clouds	46
	Private Clouds	48
	Hybrid Clouds	49
	Alternative Deployment Models	50
	The Linthicum Model	50
	The Jericho Cloud Cube Model	51
	Expected Benefits	55
	Flexibility and Resiliency	56
	Reduced Costs	57
	Centralization of Data Storage	58
	Reduced Time to Deployment	58
	Scalability	58
	Summary	59
Chapter 3	Cloud Computing Software Security Fundamentals	61
	Cloud Information Security Objectives	62
	Confidentiality, Integrity, and Availability	63
	Confidentiality	63
	Integrity	64
	Availability	64
	Cloud Security Services	64
	Authentication	64
	Authorization	64
	Auditing	65
	Accountability	66
	Relevant Cloud Security Design Principles	66
	Least Privilege	67
	Separation of Duties	67

Defense in Depth	67
Fail Safe	68
Economy of Mechanism	68
Complete Mediation	68
Open Design	69
Least Common Mechanism	69
Psychological Acceptability	69
Weakest Link	70
Leveraging Existing Components	70
Secure Cloud Software Requirements	70
Secure Development Practices	71
Handling Data	71
Code Practices	72
Language Options	73
Input Validation and Content Injection	73
Physical Security of the System	73
Approaches to Cloud Software Requirements Engineering	74
A Resource Perspective on Cloud Software Security Requirements	75
Goal-Oriented Software Security Requirements	76
Monitoring Internal and External Requirements	77
Cloud Security Policy Implementation and Decomposition	78
Implementation Issues	79
Decomposing Critical Security Issues into Secure Cloud Software Requirements	81
NIST 33 Security Principles	85
Secure Cloud Software Testing	86
Testing for Security Quality Assurance	87
Conformance Testing	89
Functional Testing	90
Performance Testing	92
Security Testing	94
Cloud Penetration Testing	99
Legal and Ethical Implications	100
The Three Pre-Test Phases	103
Penetration Testing Tools and Techniques	105
Regression Testing	111
Cloud Computing and Business Continuity Planning/Disaster Recovery	113
Definitions	113
General Principles and Practices	114
Disaster Recovery Planning	114
Business Continuity Planning	117
Using the Cloud for BCP/DRP	119

	Redundancy Provided by the Cloud	119
	Secure Remote Access	120
	Integration into Normal Business Processes	120
	Summary	120
Chapter 4	Cloud Computing Risk Issues	125
	The CIA Triad	125
	Confidentiality	125
	Integrity	126
	Availability	126
	Other Important Concepts	127
	Privacy and Compliance Risks	127
	The Payment Card Industry Data Security Standard (PCI DSS)	128
	Information Privacy and Privacy Laws	130
	Threats to Infrastructure, Data, and Access Control	141
	Common Threats and Vulnerabilities	141
	Logon Abuse	143
	Inappropriate System Use	143
	Eavesdropping	143
	Network Intrusion	144
	Denial-of-Service (DoS) Attacks	144
	Session Hijacking Attacks	144
	Fragmentation Attacks	145
	Cloud Access Control Issues	145
	Database Integrity Issues	146
	Cloud Service Provider Risks	147
	Back-Door	148
	Spoofing	148
	Man-in-the-Middle	148
	Replay	148
	TCP Hijacking	149
	Social Engineering	149
	Dumpster Diving	149
	Password Guessing	150
	Trojan Horses and Malware	150
	Summary	151
Chapter 5	Cloud Computing Security Challenges	153
	Security Policy Implementation	154
	Policy Types	154
	Senior Management Statement of Policy	155
	Regulatory Policies	155
	Advisory Policies	155
	Informative Policies	155
	Computer Security Incident Response Team (CSIRT)	156

	Virtualization Security Management	157
	Virtual Threats	158
	Hypervisor Risks	163
	Increased Denial of Service Risk	164
	VM Security Recommendations	165
	Best Practice Security Techniques	165
	VM-Specific Security Techniques	169
	Hardening the Virtual Machine	169
	Securing VM Remote Access	172
	Summary	173
Chapter 6	Cloud Computing Security Architecture	177
	Architectural Considerations	178
	General Issues	178
	Compliance	178
	Security Management	179
	Information Classification	181
	Employee Termination	185
	Security Awareness, Training, and Education	186
	Trusted Cloud Computing	188
	Trusted Computing Characteristics	188
	Secure Execution Environments and Communications	191
	Secure Execution Environment	191
	Secure Communications	191
	Microarchitectures	203
	Identity Management and Access Control	204
	Identity Management	205
	Passwords	205
	Tokens	206
	Memory Cards	207
	Smart Cards	207
	Biometrics	207
	Implementing Identity Management	209
	Access Control	210
	Controls	210
	Models for Controlling Access	211
	Single Sign-On (SSO)	212
	Autonomic Security	213
	Autonomic Systems	213
	Autonomic Protection	215
	Autonomic Self-Healing	215
	Summary	216
Chapter 7	Cloud Computing Life Cycle Issues	217
	Standards	218
	Jericho Forum	218

The Distributed Management Task Force (DMTF)	219
The DMTF Open Virtualization Format (OVF)	219
The DMTF Open Cloud Standards Incubator	220
The International Organization for Standardization (ISO)	220
ISO 27001	220
ISO 27002	222
ISO 27003	222
ISO 27004	223
ISO 27005	223
ISO 27006	224
International Organization for Standardization/ International Electrotechnical Commission ISO/ IEC 29361, ISO/IEC 29362, and ISO/IEC 29363 Standards	224
Distributed Application Platforms and Services	225
The European Telecommunications Standards Institute (ETSI)	226
The Organization for the Advancement of Structured Information Standards (OASIS)	226
Storage Networking Industry Association (SNIA)	226
Open Grid Forum (OGF)	227
The Open Web Application Security Project (OWASP)	227
OWASP Top Ten Project	227
OWASP Development Guide	228
OWASP Code Review Guide	229
OWASP Testing Guide	230
Incident Response	231
NIST Special Publication 800-61	231
Preparation	232
Detection and Analysis	232
Containment, Eradication, and Recovery	233
Post-Incident Activity	234
NIST Incident-Handling Summary	234
Internet Engineering Task Force Incident-Handling Guidelines	234
Layered Security and IDS	236
Intrusion Detection	236
IDS Issues	240
Computer Security and Incident Response Teams	241
CERT/CC	242
FedCIRC	242
Forum of Incident Response and Security Teams	243
Security Incident Notification Process	243
Automated Notice and Recovery Mechanisms	244
Encryption and Key Management	246
VM Architecture	246
Key Protection Countermeasures	247
Hardware Protection	248

Software-Based Protection	249
Data Deduplication	250
Hashing	251
Retirement	252
VM Life Cycle	252
Overwriting	253
Degaussing	254
Destruction	254
Record Retention	255
Data Remanence	255
Due Care and Due Diligence	255
Documentation Control	256
Summary	256
Chapter 8 Useful Next Steps and Approaches	259
Getting Answers	259
What Services Should Be Moved to the Cloud?	260
What Questions Should You Ask Your Cloud Provider?	261
When Should You Use a Public, Private, or Hybrid Cloud?	262
Getting Help	264
Cloud Security Alliance	264
Cloud Computing Google Groups	265
Cloud Computing Interoperability Forum	266
Open Cloud Consortium	266
Getting Started	267
Top Ten List	267
1. Assess Your Data's Sensitivity	268
2. Analyze the Risks vs. Benefits of Cloud Computing	271
3. Define Business Objectives	273
4. Understand the Underlying Structure of Your Network	273
5. Implement Traditional Best Practice Security Solutions	274
6. Employ Virtualization Best Practices	274
7. Prevent Data Loss with Backups	275
8. Monitor and Audit	275
9. Seek Out Advice	276
10. Employ Deception	277
Parting Words	277
Glossary of Terms and Acronyms	279
References	345
Index	349



Foreword

Whenever we come upon something new, we try to understand it. A good way of understanding new things is to look for something from our experience that can serve as a metaphor. Sometimes this process works well, sometimes not.

Computer security has long labored under the metaphor of physical security. It stands to reason that we would assume that millennia of experience with keeping physical assets safe would serve us in keeping digital assets safe as well.

Much of our thinking in computer security has therefore been concerned with putting important things someplace “safe” and then controlling access to it. I distinctly recall a conversation with a security analyst at the beginning of the PC network era. When asked how to ensure the security of data on a PC, he said, “Simple. Put the data on the PC. Put the PC in a safe. Put the safe at the bottom of the ocean.”

We have been challenged over the years with coming up with safe places that allowed access. We have been challenged with even figuring out what “safe” might mean in a world where risks could come from anywhere, including inside our own organizations.

In today’s world, the physical security metaphor continues to deteriorate. We’ve all seen a movie or TV show where some critical piece of data becomes key to the plot. The location of the next terrorist attack is kept on a single USB that is subject to theft, deterioration, or any other number of physical ills designed to increase the drama. That is simply not the nature of data. Data is viral. Where did this data come from? It was never on a hard drive? No one ever emailed anybody about the attack? Can’t somebody plug the damn key in and make a YouTube video about it so that everyone can see it?

As we move to this new era of cloud computing, the last vestiges of our physical world metaphors are swept away. We need to understand data access

and validation in a new way — perhaps in the way they should have been understood all along. Data security needs to be understood as something new, requiring new and innovative solutions.

Security professionals are perhaps rightfully overwhelmed by this challenge. Despite increased spending, the average firm finds itself less secure than it was five years ago. Advancements in security tools and techniques have not kept pace with risks and attack vectors. How can the security community respond to these ever-increasing threats when the additional requirements of virtualization and agility drive data assets up into a nebulous “cloud”?

One thing we do know for sure: Security will not drive or control this change. Any business requirement for lower costs and increased agility of cloud computing will eventually rule the day. Security professionals have attempted to slow the growth of several technology initiatives over the years in an attempt to control the risks. E-mail, instant messaging, and web browsing are some that come to mind immediately. We know from past experience, however, that implementing appropriate controls generally works far better than attempting to simply stop these initiatives.

As security professionals, it is incumbent on us to generate innovations in our concepts of data security and integrity. We need tools and processes that recognize the ephemeral nature of data and the reality that physical locational controls simply will not work going forward. With a little hard work, we can achieve security models that minimize risk and enable this new method of computing. We don’t need to give up on security; we simply need to abandon some of our metaphors.

This book serves as a guide for doing just that. As security professionals, we may not want to embrace the cloud, but we’re certainly going to have to learn to live with it.

Ken Phelan
CTO Gotham Technology Group



Introduction

Cloud computing provides the capability to use computing and storage resources on a metered basis and reduce the investments in an organization's computing infrastructure. The spawning and deletion of virtual machines running on physical hardware and being controlled by hypervisors is a cost-efficient and flexible computing paradigm.

In addition, the integration and widespread availability of large amounts of "sanitized" information such as health care records can be of tremendous benefit to researchers and practitioners.

However, as with any technology, the full potential of the cloud cannot be achieved without understanding its capabilities, vulnerabilities, advantages, and trade-offs. This text provides insight into these areas and describes methods of achieving the maximum benefit from cloud computation with minimal risk.

Overview of the Book and Technology

With all its benefits, cloud computing also brings with it concerns about the security and privacy of information extant on the cloud as a result of its size, structure, and geographical dispersion. Such concerns involve the following issues:

- Leakage and unauthorized access of data among virtual machines running on the same server
- Failure of a cloud provider to properly handle and protect sensitive information

- Release of critical and sensitive data to law enforcement or government agencies without the approval and/or knowledge of the client
- Ability to meet compliance and regulatory requirements
- System crashes and failures that make the cloud service unavailable for extended periods of time
- Hackers breaking into client applications hosted on the cloud and acquiring and distributing sensitive information
- The robustness of the security protections instituted by the cloud provider
- The degree of interoperability available so that a client can easily move applications among different cloud providers and avoid “lock-in”

Cloud users should also be concerned about the continued availability of their data over long periods of time and whether or not a cloud provider might surreptitiously exploit sensitive data for its own gain.

One mitigation method that can be used to protect cloud data is encryption. Encrypting data can protect it from disclosure by the cloud provider or from hackers, but it makes it difficult to search or perform calculations on that data.

This book clarifies all these issues and provides comprehensive guidance on how to navigate the field of cloud computing to achieve the maximum return on cloud investments without compromising information security.

How This Book Is Organized

The text explores the principal characteristics of cloud computing, including scalability, flexibility, virtualization, automation, measured service, and ubiquitous network access, while showing their relationships to secure cloud computing.

The book chapters proceed from tracing the evolution of the cloud paradigm to developing architectural characteristics, security fundamentals, cloud computing risks and threats, and useful steps in implementing secure cloud computing.

Chapter 1 defines cloud computing and provides alternative views of its application and significance in the general world of computing. Following this introduction, the chapter presents the essential characteristics of cloud computing and traces the historical architectural, technical, and operational influences that converged to establish what is understood as cloud computing today.

Chapter 2 looks at the primary elements of the cloud computing architecture using various cloud-based computing architecture models. In this chapter we'll examine cloud delivery models (the SaaS, PaaS, and IaaS elements of the SPI framework), cloud deployment models (such as private, community, public, and hybrid clouds), and look at some alternative cloud architecture models, such as the Jericho Cloud Cube.

Chapter 3 explores the fundamental concepts of cloud computing software security, covering cloud security services, cloud security principles, secure software requirements, and testing concepts. It concludes by addressing cloud business continuity planning, disaster recovery, redundancy, and secure remote access.

Chapter 4 examines cloud computing risks and threats in more detail. We'll examine cloud computing risk to privacy assurance and compliance regulations, how cloud computing presents a unique risk to "traditional" concepts of data, identity, and access management (IAM) risks, and how those risks and threats may be unique to cloud service providers (CSPs).

Chapter 5 helps identify management challenges and opportunities. Security management must be able to determine what detective and preventative controls exist to clearly define the security posture of the organization, especially as it relates to the virtualization perimeter. We'll look at security policy and computer intrusion detection and response implementation techniques, and dive deeply into virtualization security management issues.

Chapter 6 addresses the important cloud computing security architectural issues, including trusted cloud computing, secure execution environments, and microarchitectures. It also expands on the critical cloud security principles of identity management and access control and develops the concepts of autonomic systems and autonomic protection mechanisms.

Chapter 7 presents cloud life cycle issues, together with significant standards efforts, incident response approaches, encryption topics, and considerations involving retirement of cloud virtual machines and applications.

Chapter 8 recaps the important cloud computing security concepts, and offers guidance on which services should be moved to the cloud and those that should not. It also reviews questions that a potential user should ask a cloud provider, and lists organizations that provide support and information exchange on cloud applications, standards, and interoperability. Chapter 8 concludes with advice on getting started in cloud computation and a "top ten" list of important related considerations.

Who Should Read This Book

Cloud Security: A Comprehensive Guide to Secure Cloud Computing is designed to be a valuable source of information for those who are contemplating using cloud computing as well as professionals with prior cloud computing experience and knowledge. It provides a background of the development of cloud computing and details critical approaches to cloud computing security that affect the types of applications that are best suited to the cloud.

We think that *Cloud Security: A Comprehensive Guide to Secure Cloud Computing* would be a useful reference for all of the following:

- Professionals working in the fields of information technology or information system security
- Information security audit professionals
- Information system IT professionals
- Computing or information systems management
- Senior management, seeking to understand the various elements of security as related to cloud computing
- Students attending information system security certification programs or studying computer security

Summary

We hope *Cloud Security: A Comprehensive Guide to Secure Cloud Computing* is a useful and readable reference for everyone concerned about the risk of cloud computing and involved with the protection of data.

Issues such as data ownership, privacy protections, data mobility, quality of service and service levels, bandwidth costs, data protection, and support have to be tackled in order to achieve the maximum benefit from cloud computation with minimal risk.

As you try to find your way through a maze of security minefields, this book is mandatory reading if you are involved in any aspect of cloud computing.

Cloud Computing Fundamentals

Out of intense complexities intense simplicities emerge.

—Winston Churchill

Cloud computing evokes different perceptions in different people. To some, it refers to accessing software and storing data in the “cloud” representation of the Internet or a network and using associated services. To others, it is seen as nothing new, but just a modernization of the time-sharing model that was widely employed in the 1960s before the advent of relatively lower-cost computing platforms. These developments eventually evolved to the client/server model and to the personal computer, which placed large amounts of computing power at people’s desktops and spelled the demise of time-sharing systems.

In 1961, John McCarthy, a professor at MIT, presented the idea of computing as a utility much like electricity.¹ Another pioneer, who later developed the basis for the ARPANET, the Department of Defense’s Advanced Research Projects Agency Network, and precursor to the Internet, was J.C.R. Licklider. In the 1960s, Licklider promulgated ideas at both ARPA and Bolt, Beranek and Newman (BBN), the high-technology research and development company, that envisioned networked computers at a time when punched card, batch computing was dominant. He stated, “If such a network as I envisage nebulously could be brought into operation, we could have at least four large computers, perhaps six or eight small computers, and a great assortment of disc files and magnetic tape units—not to mention remote consoles and teletype stations—all churning away.”²

The conjunction of the concepts of utility computing and a ubiquitous world-wide network provided the basis for the future evolution of cloud computing.

What Is Cloud Computing?

In an October, 2009 presentation titled “Effectively and Securely Using the Cloud Computing Paradigm,”³ by Peter Mell and Tim Grance of the National Institute of Standards and Technology (NIST) Information Technology Laboratory, cloud computing is defined as follows:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction.

This cloud model is composed of five essential characteristics, three service models, and four deployment models. The five essential characteristics are as follows:

- On-demand self-service
- Ubiquitous network access
- Resource pooling
- Location independence
- Rapid elasticity
- Measured service

The service models are as follows:

- Cloud Software as a Service (SaaS)—Use provider’s applications over a network.
- Cloud Platform as a Service (PaaS)—Deploy customer-created applications to a cloud.
- Cloud Infrastructure as a Service (IaaS)—Rent processing, storage, network capacity, and other fundamental computing resources.

The deployment models, which can be either internally or externally implemented, are summarized in the NIST presentation as follows:

- Private cloud—Enterprise owned or leased
- Community cloud—Shared infrastructure for specific community
- Public cloud—Sold to the public, mega-scale infrastructure
- Hybrid cloud—Composition of two or more clouds

These characteristics and models are covered in detail in Chapter 2.