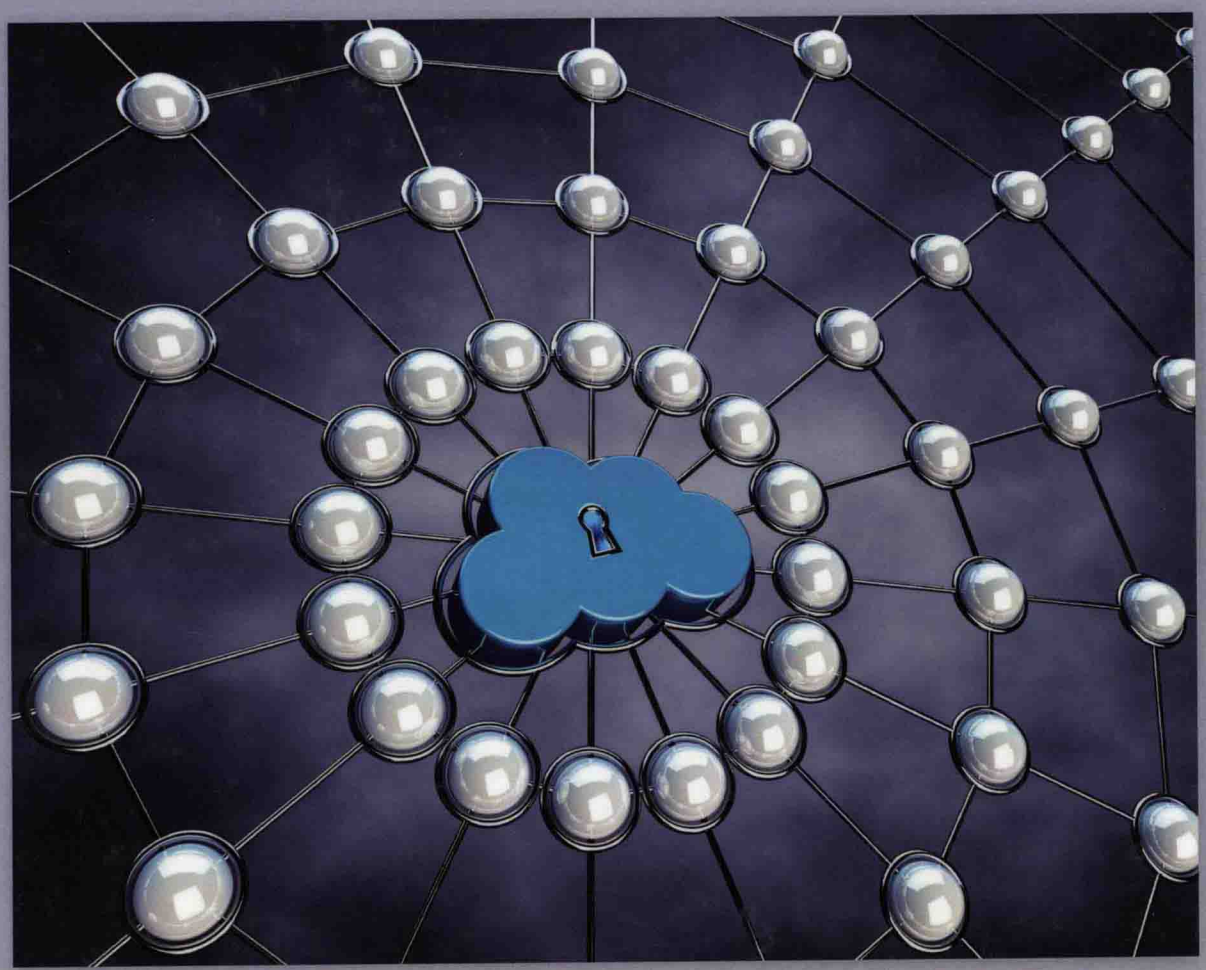
PREMIER REFERENCE SOURCE

Security Engineering for Cloud Computing

Approaches and Tools



David G. Rosado, Daniel Mellado,
Eduardo Fernandez-Medina & Mario Piattini

Security Engineering for Cloud Computing:

Approaches and Tools

David G. Rosado
University of Castilla-La Mancha, Spain

Daniel Mellado
Rey Juan Carlos University, Spain

Eduardo Fernandez-Medina
University of Castilla-La Mancha, Spain

Mario Piattini
University of Castilla-La Mancha, Spain

Information Science
REFERENCE

Managing Director: Lindsay Johnston
Editorial Director: Joel Gamon
Book Production Manager: Jennifer Romanchak
Publishing Systems Analyst: Adrienne Freeland
Development Editor: Myla Merkel
Assistant Acquisitions Editor: Kayla Wolfe
Typesetter: Deanna Jo Zombro
Cover Design: Nick Newcomer

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Security engineering for cloud computing : approaches and tools / David G. Rosado, Daniel Mellado, Eduardo Fernandez-Medina, and Mario Piattini, editors.
pages cm
Includes bibliographical references and index.
Summary: "This book provides a theoretical and academic description of Cloud security issues, methods, tools and trends for developing secure software for Cloud services and applications"-- Provided by publisher.
ISBN 978-1-4666-2125-1 (hardcover) -- ISBN 978-1-4666-2127-5 (print & perpetual access) -- ISBN (invalid) 978-1-4666-2126-8 (ebook) 1. Cloud computing--Security measures. 2. Computer security. 3. Data protection. 4. Computer networks--Security measures. I. Rosado, David G., 1977-
QA76.585.S44 2013
005.8--dc23

2012025271

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Editorial Advisory Board

List of Reviewers

Foreword

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

Although the adoption of Cloud computing brings many benefits, security is considered to be a significant barrier to this adoption. Organizations and individuals are often concerned about how security, privacy, and integrity can be maintained in this new environment. The security engineering that is applied to Cloud computing is therefore a fundamental aspect if a systematic, disciplined, secure approach to the development, operation, and maintenance of software is to be obtained. The security engineering that is focused on migration approaches of legacy systems is also a fundamental aspect in the adoption of Cloud computing by organizations and companies who additionally wish to migrate the security aspects of their existing applications and systems.

There are numerous security challenges in Cloud Computing that must be researched and studied, such as access control and user authentication, regulatory compliance, legal issues, data safety, data separation and data segregation, business continuity, recovery, lack of control, lack of visibility, lack of manageability, loss of governance, compliance risk, isolation failure, data protection, management interfaces and access configuration, and integration with internal security. This book covers many of the challenges related to the security of Cloud computing which have been written by internationally recognized leaders in this field, and the importance of and need for research into security for Cloud computing is evident in each chapter.

The first section of the book deals with security architectures, the security aspects and properties to be considered in these cloud architectures, and misuse patterns for Cloud environments.

The second section takes a look at existing risks and vulnerabilities in Cloud Computing, and at various risk analysis and management approaches for this kind of systems.

The third section of the book is focused, on the one hand, on hardware security and secure storage and, on the other, on policy management in the Cloud.

This book is therefore recommended for practitioners and researchers working in Cloud computing security. The various topics presented in this book open a wide range of possibilities from a researcher's point of view, with numerous references and attractive proposals. The readers can discover the state–of-the-art and importance of security in Cloud computing and understand what the main vulnerabilities, attacks, and risks are in order to propose security solutions, tools, mechanisms, services or standards

with which to solve and avoid these issues. This book can also help its readers to make decisions about which security aspects, requirements, services, or mechanisms should be taken into account if they wish to migrate their applications or systems to the Cloud or develop them in Cloud development platforms.

Rajkumar Buyya
The University of Melbourne, Australia

Rajkumar Buyya *is Director of the Cloud Computing and Distributed Systems Laboratory in the Department of Computing and Information Systems at the University of Melbourne, Australia. His research objective is to innovate and advance the field of Internet-based distributed computing, software engineering, grid and cloud computing, and its e-science and e-business applications with distinction. His research interests also include network-based computer architecture and operating systems, parallel and distributed computing systems (cluster, grid, cloud, and peer-to-peer systems), utility computing, and internet-scale service-oriented software engineering. He earned his PhD from Monash University, his Master of Engineering from Bangalore University, and his Bachelor of Engineering from University of Mysore, all in Computer Science and Engineering.*

Preface

Cloud Engineering is a multidisciplinary method which is focused on Cloud services and encompasses contributions from diverse areas such as software engineering and security engineering. The incorporation of security into engineering processes, and the application of security engineering ensure that Cloud systems have been analyzed, designed, built, tested, deployed, and developed in the most reliable, correct, robust, and secure manner.

The need to investigate and propose security solutions for Cloud Computing is therefore justified in order to ensure and improve the quality and security of all services, applications, tools, and models based on Cloud computing. This requires the analysis and in-depth study of how security in software engineering can be used and managed for Cloud Computing. The development and modelling of security from the first phases of the development of Cloud systems makes is possible to obtain more robust and secure Cloud systems.

CLOUD COMPUTING

The global presence of the Internet and the introduction of the wireless networking and mobile devices that always feature in Internet connectivity have raised user expectations and their demands for services from the Internet. However, the architectures required by service providers to enable Web 2.0 have created an IT service that is differentiated by its resilience, scalability, reusability, interoperability, security, and open platform development. This has effectively become the backbone of Cloud Computing and is considered by a number of vendors and services to be an operating system layer of its own (CPNI, Centre for the Protection of National Infrastructure 2010). Cloud Computing appears as both a computational model or paradigm and a distribution architecture, and its principal objective is to provide secure, quick, convenient data storage, and net computing services, with all computing resources being visualized as services and delivered via the Internet (Zhao, Liu, et al. 2009; Zhang, Zhang, et al. 2010). The Cloud enhances collaboration, agility, scaling, and availability, the ability to scale to fluctuations according to demand and accelerate development work, and provides the potential for cost reduction through optimized and efficient computing (Cloud Security Alliance 2009; Marinos and Briscoe 2009; CPNI, Centre for the Protection of National Infrastructure 2010; Khalid 2010).

The importance of Cloud Computing is increasing, and it is receiving growing attention in the scientific community. A study by Gartner (Gartner 2011) considers Cloud Computing to be one of the top 10 most important technologies, with a better prospect in 2013 and successive years for companies and organizations.

Cloud Computing combines a number of computing concepts and technologies such as SOA, Web 2.0, virtualization, and other technologies that rely on the Internet, thus providing common business applications online through Web browsers to satisfy users' computing needs, while the software and data are stored on the servers (Marinos and Briscoe 2009). These technologies have allowed Cloud customer organizations to achieve an improved utilization and efficiency of their service providers' infrastructure and, greater flexibility when scaling IT services up and down. In some respects, Cloud Computing represents the maturing of these technologies and is a marketing term with which to represent this maturity and the Cloud services provided (CPNI. Centre for the Protection of National Infrastructure 2010). There is commercial pressure on businesses to adopt Cloud Computing models. However, customers need to ensure that their Cloud services are driven by their own business needs rather than by providers' interests, which will be driven by short-term revenues and sales targets and long-term market share aspirations (CPNI. Centre for the Protection of National Infrastructure 2010; Rittinghouse and Ransome 2010).

NIST (NIST 2009) defines Cloud Computing as a model with which to enable convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The essential characteristics are (NIST 2009; CPNI. Centre for the Protection of National Infrastructure 2010):

- **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed, and automatically without requiring human interaction with each service provider.
- **Broad network access:** Capabilities are available over the network and are accessed through standard mechanisms that promote use through heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources that are dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control over or knowledge of the exact location of the resources provided but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, in order to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the service utilized.
- **Pay per use:** Capabilities are charged using a metered, fee-for-service, or advertising based billing model to promote optimization of resource use. Examples are: measuring the storage, bandwidth, and computing resources consumed, and charging for the number of active user accounts per month. Clouds within an organization accrue costs between business units and may or may not use actual currency.

TYPES OF CLOUD MODELS

This Cloud model promotes availability and is composed of three service models (NIST 2009; Zhang, Cheng et al. 2010; Subashini and Kavitha 2011):

- **Cloud Software as a Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a Cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email). SaaS refers to providing on demand applications over the Internet.
- **Cloud Platform as a Service (PaaS):** The capability provided to the consumer is to deploy on the Cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services.
- **Cloud Infrastructure as a Service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. IaaS refers to on-demand provisioning of infrastructural resources, usually in terms of Virtual Machines (VMs).

There are three types of cloud deployment models available. However, there are is another type of cloud deployment model known as Community Cloud which is also being used in some instances (NIST 2009):

- **Private Cloud:** The Cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on or off the premises.
- **Community Cloud:** The Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on or off the premises.
- **Public Cloud:** The Cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling Cloud services.
- **Hybrid Cloud:** The Cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

SECURITY IN CLOUD COMPUTING

Although there are many benefits involved in adopting Cloud Computing, there are also some significant barriers to its adoption. One of the most significant barriers is security, followed by issues regarding compliance, privacy, and legal matters (KPMG 2010). Since Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty as to how security at all levels (e.g., network,

host, application, and data levels) can be achieved. This uncertainty has consistently led information executives to state that security is their number one concern as regards Cloud Computing (Mather, Kumaraswamy et al. 2009).

Security is the main obstacle for many organizations in their move to the Cloud, and is related to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy, and integration with internal security. Compared to traditional technologies, the Cloud has many specific features, such as the fact that it is large-scale, and that resources belonging to Cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity validation authentication and authorization are no longer suitable for the Cloud (Li and Ping 2009). Security controls in Cloud Computing are, for the most part, no different to security controls in any other IT environment. However, the Cloud service models employed, the operational models, and the technologies used to enable Cloud services signify that Cloud Computing may present an organization with different risks than those associated with traditional IT solutions. Unfortunately, integrating security into these solutions is often perceived as making them more rigid (Cloud Security Alliance 2009).

The ENISA report (ENISA 2009) highlights the benefits that some small and medium size companies can attain with Cloud Computing. A smaller, cost-constrained organization may find that a Cloud deployment allows it to take advantage of large-scale infrastructure security measures that it could not otherwise afford. Some of the possible advantages include DDOS (distributed denial of service) protection, forensic image support, logging infrastructure, timely patch and update support, scaling resilience, and perimeter protection (firewalls, intrusion detection, and prevention services).

The adoption of Cloud Computing has been increasing for some time, and the maturity of the market is steadily growing not only in volume, choice, and functionality, but also in terms of the suppliers' ability to answer the complex security, regulatory and compliance questions that security oversight functions are now asking. This growth has, in part, been driven by the continued view that Cloud services will deliver cost savings and increased flexibility (Wilson 2011).

SECURITY BENEFITS IN CLOUD COMPUTING

Although there is a significant benefit to leveraging Cloud Computing, security concerns have led organizations to hesitate to move their critical resources to the Cloud (Rittinghouse and Ransome 2010). With the Cloud model, users lose control over their physical security owing to the fact that they are sharing computing resources with other companies (with the Public Cloud) and moreover, if they should decide to move the storage services provided by one Cloud vendor's services to another, these storage services may be incompatible with another vendor's services. Moreover, data backup are critical aspects with which to facilitate recovery in the case of disaster, but this also implies security concerns (Subashini and Kavitha 2011). Another concern is related to the immature use of mashup technology (combinations of Web services), which is fundamental to Cloud applications, and will inevitably cause unwitting security vulnerabilities in these applications. It is recommendable that the development tool of choice should have a security model embedded in it to guide developers during the development phase and to restrict users only to their authorized data when the system is deployed in production (Rittinghouse and Ransome 2010; Subashini and Kavitha 2011).

Others needs that organizations and customers require from Cloud providers are that they provide log data in real-time, and that they permit the government policy to be changed in response to both the opportunity and the threats that Cloud Computing brings. This will probably focus on the off-shoring of personal data and the protection of privacy, whether the data is being controlled by a third party or is off-shored to another country. Enterprises are often required to prove that their security compliance accords with regulations, standards, and auditing practices, regardless of the location of the systems in which the data resides. Standards regulate how information security management is being implemented, managed, and conducted. Issues related to virtualization are also important for enterprises and organizations because virtualization efficiencies in the Cloud require virtual machines from multiple organizations to be co-located in the same physical resources, and the dynamic and fluid nature of virtual machines will therefore make it difficult to maintain the consistency of security and ensure the auditability of records (Onwubiko 2010; Rittinghouse and Ransome 2010).

In the rush to take advantage of the benefits of Cloud Computing, not least of which is significant cost savings, many corporations are probably rushing into Cloud Computing without a serious consideration of the security implications. In order to overcome customer concerns regarding application and data security, vendors must address these issues head-on. There is a strong apprehension about insider breaches, along with vulnerabilities in the applications and the systems' availability that could lead to a loss of sensitive data and money. Such challenges may dissuade enterprises from adopting applications within the Cloud (Subashini and Kavitha 2011). The focus is not therefore upon the portability of applications, but on preserving or enhancing the security functionality provided by the legacy application and achieving a successful application migration (Cloud Security Alliance 2009).

The Cloud providers and vendors have advanced in this direction by improving the security aspects and solutions which are offered to those customers who wish to move their applications and data to the Cloud, thus making it a very attractive paradigm owing to its perceived economic and operational benefits. Cloud Computing offers a set of security benefits for Cloud applications but a cause of concern is how enterprises can migrate their security requirements in such a way that they will fit with the Cloud security solutions, and how the security of their applications and data will be maintained and managed.

Within this attractive set of benefits we can find the security benefits that are offered by the Cloud providers to those of their customers who choose to move their applications to the Cloud (ENISA 2009; Velte, Toby J. Velte et al. 2010; Jansen and Grance 2011). Of the most popular security benefits in Cloud Computing, we can define the following:

- **Security and the benefits of scale:** put simply, all kinds of security measures are cheaper when implemented on a larger scale.
- **Security as a market differentiator:** security is a priority concern for many Cloud customers; many of them will make buying choices on the basis of the reputation for confidentiality, integrity and resilience of, and the security services offered by a provider.
- **Standardised interfaces for managed security services:** large Cloud providers can offer a standardised, open interface with which to manage security services providers. This creates a more open and readily available market for security services.
- **Rapid, smart scaling of resources:** the ability of the Cloud provider to dynamically reallocate resources for filtering, traffic shaping, authentication, encryption, et cetera, to defensive measures (e.g., against DDoS attacks) has obvious advantages for resilience.

In addition to these benefits, the Cloud also has other benefits such as more timely and effective and efficient updates and defaults; there are some good security traits that come with the centralization of data; Cloud providers have the opportunity to permit their staff to specialize in security, privacy and other areas of great interest and concern to the organization; the structure of Cloud Computing platforms is typically more uniform than that of most traditional computing centres; greater uniformity and homogeneity facilitate platform hardening and enable better automation of security management activities such as configuration control, vulnerability testing, security audits, and security patching of platform components resource availability; backup and recovery; redundancy and disaster recovery capabilities are built into Cloud Computing environments and on-demand resource capacity can be used for better resilience when confronting increased service demands or distributed denial of service attacks, and for quicker recovery from serious incidents; the architecture of a Cloud solution extends to the client at the service endpoint, and is used to access hosted applications; data maintained and processed in the cloud are not such a great risk to an organization with a mobile workforce as that data being dispersed on portable computers or removable media out in the field, where the theft and loss of devices routinely occur.

AIMS OF THIS BOOK

This book attempts to provide a general knowledge base on a wide range of issues related to security in software engineering oriented towards Cloud systems, in order to show the existing problems and challenges, to show what initiatives are being carried out, to propose security approaches and any aspect of security that might be of interest to both academia and the research world, and business and social environments.

This book aims to provide a theoretical and academic description of Cloud security issues, methods, methodologies, models, architectures, designs, tools, services, techniques, challenges, and trends for developing secure software for Cloud infrastructures, platforms, services, or applications.

The book covers the following topics:

- An in-depth review of the most common vulnerabilities and attacks confronted by Cloud Computing.
- Approaches based on Security in Cloud Architectures and Misuse patterns.
- Techniques for the monitoring of security properties in Cloud Computing scenarios, analysis models of risk analyses, and goal-driven risk management.
- Hardware-based security mechanisms and data availability, integrity and confidentiality techniques for a virtualization middleware.
- Access control systems and Policy management in Cloud Computing environments.

Target Audience

The proposed book could serve as a reference for:

- CEOs and CIOs
- Security managers
- Systems specialists and architects

- Security developers
- Information security professionals
- Computer Science students.

ORGANIZATION OF THIS BOOK

This book is divided into three sections and ten chapters. Each section addresses a state-of-the-art topic concerning Security in Cloud Computing, and are as follows: *Cloud Architecture and Patterns, Risks and vulnerabilities in Cloud Computing,* and *Hardware Security, Secure Storage, and Policy Management in Cloud.*

Section 1: Cloud Architecture and Patterns

Chapter 1: *Dynamic Security Properties Monitoring Architecture for Cloud Computing*

In this chapter the authors provide an overview of the importance of the monitoring of security properties in Cloud Computing scenarios. They also present an approach based on the monitoring of security properties in Cloud systems, which is based on a diagnosis framework that supports the specification and monitoring of properties expressed in Event Calculus (EC) as rules as the basis. The provision of diagnosis information is based on the generation of alternative explanations for the events that are involved in the violations of rules. This approach is based on Virtualization Architectures, which have several threats that have been identified in the instrumentation of Virtualized Environments.

Chapter 2: *The SeCA model: Ins and Outs of a Secure Cloud Architecture*

This chapter outlines the Secure Cloud Architecture (SeCA) model on the basis of data classifications, which defines a properly secure Cloud architecture by testing the Cloud environment as regards eight attributes. The SeCA model is developed by using a literature review and a Delphi study with seventeen experts, consisting of three rounds. The authors integrate the CI3A, an extension on the CIA-triad, to create a basic framework with which to test the classification inputted. The data classification is then tested on regional, geo-spatial, delivery, deployment, governance & compliance, and network and premise attributes. After this testing has been executed, a specification for a secure Cloud architecture is outputted. The SeCA model is detailed with two example cases concerning the usage of the model in practice.

Chapter 3: *Three Misuse Patterns for Cloud Computing*

The purpose of this chapter is to describe certain attacks in the form of misuse patterns, where a misuse pattern describes how an attack is performed from the point of view of the attacker. The authors describe three misuse patterns in particular: Resource Usage Monitoring Inference, Malicious Virtual Machine Creation, and Malicious Virtual Machine Migration Process.

Section 2: Risks and Vulnerabilities in Cloud Computing

Chapter 4: *Security Risks in Cloud Computing: An Analysis of the Main Vulnerabilities*

The recent and continuous appearance of vulnerabilities in software systems makes security a vital issue if these systems are to succeed. The purpose of this chapter is to provide an analysis of the most common vulnerabilities in recent years, focusing on those vulnerabilities which are specific

to Cloud Computing. These specific vulnerabilities need to be identified in order to avoid them by providing prevention mechanisms, and the following questions have therefore been posed: What kinds of vulnerabilities are increasing? Has any kind of vulnerability been reduced in recent years? What is the evolution of their severity?

Chapter 5: *A Software Tool to Support Risks Analysis about what Should or Shouldn't go to the Cloud*

This chapter proposes a software prototype called *2thecloud*, programmed in HTML and PHP under free software guidelines, whose main objective is to allow end users to be aware of imminent dangers in the Cloud. To do this, the user must undergo a metacognitive process of basic risk analysis, whose suggested result would be to which cloud the object should go. It is supposed that the user can use this tool to develop a risk analysis capability, such that it is the user who makes the final decision concerning the selection of the cloud model (public, private, hybrid and Community) in which the object will be placed. The authors finally propose four alternatives in risk analysis calculation, which are plausibly adapted to *2thecloud*.

Chapter 6: *A Goal-Driven Risk Management Approach to Support Security and Privacy Analysis of Cloud-Based Systems*

In this chapter, the authors propose a goal-driven risk management modeling (GSRM) framework, with which to assess and manage risks, that supports analysis from the early stages of Cloud-based systems development. The approach explicitly identifies the goals that the system must fulfill, and the potential risk factors that obstruct the goals, so that suitable control actions can be identified to control such risks. The authors provide an illustrative example of the application of the proposed approach in an industrial case study in which a Cloud service is deployed to share data amongst project partners.

Chapter 7: *Real Time Risk Management in Cloud Computation*

This chapter reviews the potential vulnerabilities of Cloud-based architectures and uses this as the foundation to define a set of requirements for reassessing risk management in Cloud Computing. In order to fulfill these requirements, the authors propose a new scheme for the real-time assessment and auditing of risk in Cloud-based applications and explore this with the use case of a triage application.

Section 3. Hardware Security and Secure Storage and Policy Management in Cloud

Chapter 8: *Hardware-based Security for Ensuring Data Privacy in the Cloud*

The purpose of this chapter is to present a set of hardware-based security mechanisms with which to ensure the privacy, integrity, and legal compliance of customer data as it is stored and processed in the Cloud. The security system presented leverages the tamper-proof capabilities of cryptographic coprocessors to establish a secure execution domain in the Cloud computing that is physically and logically protected from unauthorized access. The main design goal is to maximize users' control in managing the various aspects related to the privacy of sensitive data by implementing user-configurable software protection and data privacy categorization mechanisms.

Chapter 9: *Securing Cloud Storage*

Data storage appears as a central component of the problem associated with moving processes and resources in the Cloud. Whether it is a simple storage externalization for backup purposes, the use of hosted software services, or virtualization in a third-party provider of the company computing

infrastructure, data security is crucial. This security declines according to three axes: data availability, integrity, and confidentiality. Numerous techniques targeting these three issues exist, but none presents the combined guarantees that would allow a practical implementation. In this chapter, the authors present a solution for the integration of these techniques into a virtualization middleware. A definition of the quality of service allows the specification of the nature of the security to be implemented with a seamless access.

Chapter 10: *Policy Management in Cloud: Challenges and Approaches*

In this chapter, the authors discuss access control systems and policy management in Cloud Computing environments. Cloud computing environments may not permit the use of a single access control system, single policy language, or single management tool for the various Cloud services that they offer. Access control policies may be composed in incompatible ways as a result of the diverse policy languages that are maintained separately by every Cloud provider. Heterogeneity and the distribution of these policies create problems in managing access policy rules for a Cloud environment. In this chapter, the authors discuss the challenges of policy management and introduce a Cloud based policy management framework that is designed to give users a unified control point with which to manage access policies in order to control access to their resources, no matter where they are stored.

David G. Rosado
University of Castilla-La Mancha, Spain

Daniel Mellado
Rey Juan Carlos University, Spain

Eduardo Fernández-Medina
University of Castilla – La Mancha, Spain

Mario Piattini
University of Castilla – La Mancha, Spain

REFERENCES

Cloud Security Alliance. (2009). *Security guidance for critical areas of focus in cloud computing* V2.1.

CPNI, Centre for the Protection of National Infrastructure. (2010). *Information security briefing 01/2010.* Cloud Computing.

ENISA. (2009). *Cloud computing: Benefits, risks and recommendations for information security. D. C. a. G.* Hogben, European Network and Information Security Agency.

Gartner. (2011). *Gartner identifies the top 10 strategic technologies for 2012.*

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

Khalid, A. (2010). Cloud computing: Applying issues in small business. *International Conference on Signal Acquisition and Processing*, (pp. 278-281).

KPMG. (2010). *From hype to future*. KPMG's 2010 Cloud Computing Survey.

Li, W., & Ping, L. (2009). *Trust model to enhance security and interoperability of cloud environment.* 1st International Conference on Cloud Computing (CloudCom), Beijing, China.

Marinos, A., & Briscoe, G. (2009). *Community cloud computing*. 1st International Conference on Cloud Computing (CloudCom), Beijing, China.

Mather, T., & Kumaraswamy, S. (2009). *Cloud security and privacy*. O'Reilly Media, Inc.

Mell, P., & Grance, T. (2009). *The NIST definition of cloud computing*. National Institute of Standards and Technology.

Onwubiko, C. (2010). Security issues to cloud computing. In Antonopoulos, N., & Gillam, L. (Eds.), *Cloud computing: Principles, systems and applications*. Springer Verlag. doi:10.1007/978-1-84996-241-4_16

Rittinghouse, J. W., & Ransome, J. F. (Eds.). (2010). *Cloud computing implementation, management, and security*. CRC Press.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11. doi:10.1016/j.jnca.2010.07.006

Velte, A. T., Toby, P. D., & Velte, J. (2010). *Cloud computing: A practical approach*. McGraw-Hill.

Wilson, P. (2011). *Positive perspectives on cloud security* (pp. 1-5). Information Security Technical Report.

Zhang, Q., & Cheng, L. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, *1*, 7–18. doi:10.1007/s13174-010-0007-6

Zhang, S., Zhang, S., et al. (2010). *Cloud computing research and development trend.* Second International Conference on Future Networks, Sanya, Hainan, China.

Zhao, G., Liu, J., et al. (2009). *Cloud computing: A statistics aspect of users*. 1st International Conference on Cloud Computing (CloudCom), Beijing, China.

Section 1
Cloud Architecture and Patterns