1.

Record Nr.	UNINA9910298573503321
Titolo	Secure Cloud Computing / / edited by Sushil Jajodia, Krishna Kant, Pierangela Samarati, Anoop Singhal, Vipin Swarup, Cliff Wang
Pubbl/distr/stampa	New York, NY : , : Springer New York : , : Imprint : Springer, , 2014
ISBN	1-4614-9278-5
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (351 p.)
Disciplina	004 004.6 004.6782 005.7
Soggetti	Computer security Application software Computer communication systems Computers Systems and Data Security Information Systems Applications (incl. Internet) Computer Communication Networks Information Systems and Communication Service
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references at the end of each chapters.
Nota di contenuto	Cryptographic Key Management Issues and Challenges in Cloud Services -- Costs and Security in Clouds -- Hardware-enhanced Security for Cloud Computing -- Cloud Computing Security: What Changes with Software-Defined Networking? -- Proof of Isolation for Cloud Storage -- Selective and Fine-Grained Access to Data in the Cloud -- Enabling Collaborative Data Authorization Between Enterprise Clouds -- Making Query Execution Over Encrypted Data Practical -- Privacy-preserving Keyword Search over Encrypted Data in Cloud Computing -- Towards Data Confidentiality and a Vulnerability Analysis Framework for Cloud Computing -- Secure Mission-Centric Operations in Cloud Computing -- Computational Decoys for Cloud Security -- Towards Data Confidentiality and a Vulnerability Analysis Framework

for Cloud Computing -- Software Cruising: A New Technology for Building Concurrent Software Monitor -- Controllability and Observability of Risk and Resilience in Cyber-Physical Cloud Systems.

Sommario/riassunto

This book presents a range of cloud computing security challenges and promising solution paths. The first two chapters focus on practical considerations of cloud computing. In Chapter 1, Chandramouli, Iorga, and Chokani describe the evolution of cloud computing and the current state of practice, followed by the challenges of cryptographic key management in the cloud. In Chapter 2, Chen and Sion present a dollar cost model of cloud computing and explore the economic viability of cloud computing with and without security mechanisms involving cryptographic mechanisms. The next two chapters address security issues of the cloud infrastructure. In Chapter 3, Szefer and Lee describe a hardware-enhanced security architecture that protects the confidentiality and integrity of a virtual machine’s memory from an untrusted or malicious hypervisor. In Chapter 4, Tsugawa et al. discuss the security issues introduced when Software-Defined Networking (SDN) is deployed within and across clouds. Chapters 5-9 focus on the protection of data stored in the cloud. In Chapter 5, Wang et al. present two storage isolation schemes that enable cloud users with high security requirements to verify that their disk storage is isolated from some or all other users, without any cooperation from cloud service providers. In Chapter 6, De Capitani di Vimercati, Foresti, and Samarati describe emerging approaches for protecting data stored externally and for enforcing fine-grained and selective accesses on them, and illustrate how the combination of these approaches can introduce new privacy risks. In Chapter 7, Le, Kant, and Jajodia explore data access challenges in collaborative enterprise computing environments where multiple parties formulate their own authorization rules, and discuss the problems of rule consistency, enforcement, and dynamic updates. In Chapter 8, Smith et al. address key challenges to the practical realization of a system that supports query execution over remote encrypted data without exposing decryption keys or plaintext at the server. In Chapter 9, Sun et al. provide an overview of secure search techniques over encrypted data, and then elaborate on a scheme that can achieve privacy-preserving multi-keyword text search. The next three chapters focus on the secure deployment of computations to the cloud. In Chapter 10, Oktay el al. present a risk-based approach for workload partitioning in hybrid clouds that selectively outsources data and computation based on their level of sensitivity. The chapter also describes a vulnerability assessment framework for cloud computing environments. In Chapter 11, Albanese et al. present a solution for deploying a mission in the cloud while minimizing the mission’s exposure to known vulnerabilities, and a cost-effective approach to harden the computational resources selected to support the mission. In Chapter 12, Kontaxis et al. describe a system that generates computational decoys to introduce uncertainty and deceive adversaries as to which data and computation is legitimate. The last section of the book addresses issues related to security monitoring and system resilience. In Chapter 13, Zhou presents a secure, provenance-based capability that captures dependencies between system states, tracks state changes over time, and that answers attribution questions about the existence, or change, of a system’s state at a given time. In Chapter 14, Wu et al. present a monitoring capability for multicore architectures that runs monitoring threads concurrently with user or kernel code to constantly check for security violations. Finally, in Chapter 15, Hasan Cam describes how to manage the risk and resilience of cyber-physical systems by employing controllability and observability techniques for

linear and non-linear systems.