

# Preface

Cloud computing continues to experience a rapid proliferation because of its potential advantages with respect to ease of deploying required computing capacity as needed and at a much lower cost than running an owned computing infrastructure. However, the lack of ownership brings in myriad security and privacy challenges that are quite difficult to resolve. The purpose of this book is to provide a state-of-the-art coverage of the techniques to address these issues at all levels of the stack ranging from hardware mechanisms to application level techniques. It is hoped that the book will be useful to researchers, practitioners, and students in further research on the subject and the implementation of the techniques in real-life systems.

The term cloud computing has been used for a variety of distributed computing environments including some traditional ones. For example, a computing infrastructure owned by the organization is often referred to as a “private cloud”, which may or may not be any different from a traditional virtualized data center owned by the organization. The distinction may come if multiple entities or departments within the organization share the same infrastructure, but have their own privacy, information sensitivity, and security concerns. In contrast, a “public cloud” refers to a facility owned and operated by a separate entity and available for use by any organization or individual. Ownership and operation models in between these extremes are also possible, such as a cloud intended for use by enterprises that provides more restrictive use policies, tighter security, higher availability, etc. than public clouds. Such “community clouds” have domain specific characteristics, capabilities, and vulnerabilities different from private or public clouds.

User access to the cloud infrastructure could be provided at varying levels ranging from underlying physical infrastructure controlled directly by the user all the way up to built-in software exposed to the users. Traditionally, three specific levels have been identified: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). The challenges in providing the required security and privacy vary across the levels, with lower level access resulting in more difficult challenges in protecting the resources from misuse and attacks.

In recent years, there have been numerous incidents of exposure of confidential data either accidentally or as a result of hacker attacks. Although many of these

incidents are not specific to cloud computing, the increasing adoption of cloud computing by the government and businesses has raised the specter of perhaps even more damaging information leaks in the future. For example, the Cloud Security Alliance (CSA) has identified “The Notorious Nine” cloud computing threats for 2013 that are likely to persist in the future as well (see <https://cloudsecurityalliance.org/research/top-threats/>). The most significant threats include: (a) exploitation of side-channel information by VMs to extract sensitive information about other VMs, including the cryptographic keys, (b) data loss due to accidents or physical hazards, (c) illegal access to credentials or penetration of critical entities such as hypervisor by hackers, (d) weak APIs and interfaces, (e) denial of service or other attacks using the cloud infrastructure, (f) and insider attacks (including the service or infrastructure providers). Significantly, a common theme identified in the list of threats is the vulnerabilities brought about by the solutions themselves. This is normally a result of increased complexity and hence vulnerabilities arising from software bugs and additional configuration data. For example, the keys and other parameters needed by cryptographic algorithms must themselves be managed and protected against attacks and accidental loss.

A key attribute of cloud computing is the involvement of multiple parties that provide or use the infrastructure or services. These parties could form a natural hierarchy with physical infrastructure providers at the bottom and the end users at the top. For example, a cloud computing service provider or a broker may use physical infrastructure provided by one or more lower level entities, and expose services or virtual infrastructures used by end users or application service providers. The sharing of increasingly sophisticated and larger computing infrastructures among multiple parties makes cloud computing security a very challenging undertaking. The main reasons include:

1. Lack of trust between various parties up and down the hierarchy (e.g., between the cloud service provider and the physical infrastructure provider if they are different, or between service provider and the user) and across a level (between service providers or users running on the same shared infrastructure). The trust model drives the level of information access granted among parties and protections implemented to avoid potential abuse. Some protections (e.g., encryption) may rule out certain operations within the cloud or make them very expensive.
2. Complex privacy and anonymity requirements for information exchanges between various parties. This drives mechanisms for obfuscating and restricting access to information content, a careful control of association between different pieces of information, and avoidance of attribution of information to specific parties. These requirements may dictate what data can be kept where and where the operations on the data take place.
3. Operational disruption, integrity violation, and information leaks caused by attacks that may originate not only from malicious outsiders but also from legitimate providers and users of the cloud. These aspects in turn drive the level of protection that needs to be built at various layers including physical infrastructure, communication protocols, data storage and transmission, middleware, etc.

The chapters in this book address recent advances in addressing some of these security and privacy issues. Each chapter is intended to be self-contained, although the reader is expected to have working knowledge of the security and privacy field. It is hoped that the book will fill an important need in the rapidly emerging field of cloud computing security.

Images can be viewed in color by visiting the book's web page on SpringerLink or downloading the eBook version.

Fairfax, VA, USA

Fairfax, VA, USA

Crema, Italy

Gaithersburg, MD, USA

McLean, VA, USA

Triangle Park, NC, USA

Sushil Jajodia

Krishna Kant

Pierangela Samarati

Anoop Singhal

Vipin Swarup

Cliff Wang

Secure Cloud Computing

Jajodia, S.; Kant, K.; Samarati, P.; Singhal, A.; Cohan, V.;  
Wang, C. (Eds.)

2014, XII, 343 p. 95 illus., Hardcover

ISBN: 978-1-4614-9277-1