SPRINGER BRIEFS IN COMPUTER SCIENCE

Kan Yang
Xiaohua Jia

Security for Cloud Storage Systems

Springer

SpringerBriefs in Computer Science

For further volumes:
http://www.springer.com/series/10028

Kan Yang · Xiaohua Jia

Security for Cloud Storage Systems

Springer

Kan Yang
Xiaohua Jia
Department of Computer Science
City University of Hong Kong
Kowloon
Hong Kong SAR

ISSN 2191-5768 ISSN 2191-5776 (electronic)
ISBN 978-1-4614-7872-0 ISBN 978-1-4614-7873-7 (eBook)
DOI 10.1007/978-1-4614-7873-7
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2013939832

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Cloud storage is an important service of cloud computing, which offers services for data owners to host their data in the cloud. This new paradigm of data hosting and data access services introduces two major security concerns: (1) Protection of data integrity. Data owners may not fully trust the cloud server and worry that data stored in the cloud could be corrupted or even removed. (2) Data access control. Data owners may worry that some dishonest servers give data access to unauthorized users, such that they can no longer rely on the servers to conduct data access control. In this book, we investigate the security issues in the cloud storage systems and develop secure solutions to ensure data owners the safety and security of the data stored in the cloud.

We first introduce Third-party Storage Auditing Service (TSAS), an efficient and secure dynamic auditing service to ensure the cloud data integrity in Chap. 2. In Chap. 3, we describe Attribute-Based Access Control (ABAS), a fine-grained access control scheme with efficient attribute revocation for cloud storage systems. In Chap. 4, we further present Data Access Control for Multi-Authority Cloud Storage (DAC-MACS), a data access control scheme with efficient revocation and decryption for cloud storage systems with multiple authorities.

We hope this book gives the reader an overview of the data security for cloud storage systems, and will serve as a good introductory reference to improve the security of cloud storage systems.

Hong Kong, March 2013

Kan Yang
Xiaohua Jia

Acknowledgments

The authors would like to thank Dr. Kui Ren at University at Buffalo, The State University of New York, for his valuable suggestions and comments on our works. We also would like to thank Dr. Zhen Liu at City University of Hong Kong for his help in Attribute-based Encryption.

We are also grateful for the assistance provided by Courtney Clark and the publication team at SpringerBriefs.

Contents

Chapter 1
Introduction

Abstract Cloud computing has emerged as a promising technique that greatly changes the modern IT industry. In this chapter, we first give a brief introduction to cloud storage systems. Then, we explore some security issues in cloud storage systems, including data integrity and data confidentiality. We also give an overview on how to solve these security problems.

1.1 Brief Introduction to Cloud Storage Systems

1.1.1 Cloud Computing

Cloud computing has emerged as a promising technique that greatly changes the modern IT industry. The National Institute of Standards and Technology (NIST) defined the cloud computing as follows [12].

> *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 defined as

- On-demand self-service
- Ubiquitous network access
- Resource pooling

K. Yang and X. Jia, *Security for Cloud Storage Systems*, SpringerBriefs in Computer Science, DOI: 10.1007/978-1-4614-7873-7_1,