

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



<http://www.springer.com/978-1-4614-7872-0>

Security for Cloud Storage Systems

Yang, K.; Xiaohua, J.

2014, XI, 83 p. 11 illus., Softcover

ISBN: 978-1-4614-7872-0