

# SpringerBriefs in Computer Science

## *Series Editors*

Stan Zdonik

Peng Ning

Shashi Shekhar

Jonathan Katz

Xindong Wu

Lakhmi C. Jain

David Padua

Xuemin Shen

Borko Furht

V. S. Subrahmanian

Martial Hebert

Katsushi Ikeuchi

Bruno Siciliano

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  
ISBN 978-1-4614-7872-0  
DOI 10.1007/978-1-4614-7873-7  
Springer New York Heidelberg Dordrecht London

ISSN 2191-5776 (electronic)  
ISBN 978-1-4614-7873-7 (eBook)

Library of Congress Control Number: 2013939832

© The Author(s) 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law. The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media ([www.springer.com](http://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

<b>1</b>	<b>Introduction</b>	1
1.1	Brief Introduction to Cloud Storage Systems	1
1.1.1	Cloud Computing	1
1.1.2	Cloud Storage as a Service	2
1.2	Data Security for Cloud Storage Systems	3
1.2.1	Storage Auditing as a Service	3
1.2.2	Access Control as a Service	4
	References	5
<b>2</b>	<b>TSAS: Third-Party Storage Auditing Service</b>	7
2.1	Introduction	7
2.2	Preliminaries and Definitions	9
2.2.1	Bilinear Pairing	9
2.2.2	Computational Bilinear Diffie-Hellman Assumption	9
2.2.3	Definition of System Model	10
2.2.4	Definition of Security Model	11
2.3	An Efficient and Privacy-Preserving Auditing Protocol	12
2.3.1	Overview	12
2.3.2	Algorithms for Auditing Protocol	12
2.3.3	Construction of the Privacy-Preserving Auditing Protocol	15
2.3.4	Correctness Proof	16
2.4	Secure Dynamic Auditing	17
2.4.1	Solution of Dynamic Auditing	18
2.4.2	Algorithms and Constructions for Dynamic Auditing	18
2.5	Batch Auditing for Multi-Owner and Multi-Cloud	21
2.5.1	Algorithms for Batch Auditing for Multi-Owner and Multi-Cloud	21
2.5.2	Correctness Proof	24
2.6	Security Analysis	25
2.6.1	Provably Secure Under the Security Model	25
2.6.2	Privacy-Preserving Guarantee	27
2.6.3	Proof of the Interactive Proof System	27

2.7	Performance Analysis . . . . .	28
2.7.1	Storage Overhead . . . . .	29
2.7.2	Communication Cost . . . . .	30
2.7.3	Computation Complexity . . . . .	31
2.7.4	Computation Cost of the Owner . . . . .	32
2.8	Related Work . . . . .	33
2.9	Conclusion . . . . .	36
	References . . . . .	36
<b>3</b>	<b>ABAC: Attribute-Based Access Control . . . . .</b>	<b>39</b>
3.1	Introduction . . . . .	39
3.2	Preliminary . . . . .	40
3.2.1	Access Structures . . . . .	40
3.2.2	Linear Secret Sharing Schemes . . . . .	41
3.2.3	Bilinear Pairing . . . . .	41
3.2.4	q-Parallel BDHE Assumption . . . . .	42
3.3	System and Security Model . . . . .	42
3.3.1	System Model . . . . .	42
3.3.2	Framework . . . . .	44
3.3.3	Security Model . . . . .	44
3.4	ABAC: Attribute-Based Access Control with Efficient Revocation . . . . .	45
3.4.1	Overview . . . . .	45
3.4.2	Construction of ABAC . . . . .	46
3.4.3	Attribute Revocation Method . . . . .	48
3.5	Analysis of ABAC . . . . .	51
3.5.1	Security Analysis . . . . .	51
3.5.2	Performance Analysis . . . . .	52
3.6	Related Work . . . . .	55
3.7	Conclusion . . . . .	57
	References . . . . .	57
<b>4</b>	<b>DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems . . . . .</b>	<b>59</b>
4.1	Introduction . . . . .	59
4.2	System Model and Security Model . . . . .	60
4.2.1	System Model . . . . .	60
4.2.2	DAC-MACS Framework . . . . .	62
4.2.3	Security Model . . . . .	63
4.3	DAC-MACS: Data Access Control for Multi-Authority Cloud Storage . . . . .	65
4.3.1	Overview . . . . .	65
4.3.2	Construction of DAC-MACS . . . . .	66
4.3.3	Efficient Attribute Revocation for DAC-MACS . . . . .	69

4.4	Analysis of DAC-MACS . . . . .	71
4.4.1	Comprehensive Analysis . . . . .	72
4.4.2	Security Analysis . . . . .	72
4.4.3	Performance Analysis . . . . .	77
4.5	Related Work . . . . .	79
4.6	Conclusion . . . . .	81
	References . . . . .	82