Wireless Networks

Series Editor

Xuemin Sherman Shen
University of Waterloo
Waterloo, ON, Canada

The purpose of Springer's new Wireless Networks book series is to establish the state of the art and set the course for future research and development in wireless communication networks. The scope of this series includes not only all aspects of wireless networks (including cellular networks, WiFi, sensor networks, and vehicular networks), but related areas such as cloud computing and big data. The series serves as a central source of references for wireless networks research and development. It aims to publish thorough and cohesive overviews on specific topics in wireless networks, as well as works that are larger in scope than survey articles and that contain more detailed background information. The series also provides coverage of advanced and timely topics worthy of monographs, contributed volumes, textbooks and handbooks.

More information about this series at http://www.springer.com/series/14180

Yuan Zhang • Chunxiang Xu •
Xuemin Sherman Shen

Data Security in Cloud Storage

Springer

Yuan Zhang
School of Computer Science & Engineering
University of Electronic Science
and Technology of China
Chengdu, Sichuan, China

Chunxiang Xu
School of Computer Science & Engineering
University of Electronic Science
and Technology of China
Chengdu, Sichuan, China

Xuemin Sherman Shen
Department of Electrical and Computer
Engineering
University of Waterloo
Waterloo, ON, Canada

ISSN 2366-1186 ISSN 2366-1445 (electronic)
Wireless Networks
ISBN 978-981-15-4373-9 ISBN 978-981-15-4374-6 (eBook)
https://doi.org/10.1007/978-981-15-4374-6

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

Cloud storage is a service that lets users store data by transferring it over the Internet or another network to an offsite storage system maintained by a third party. It is increasingly demanded along the users' data exploded and it provides users an efficient and convenient way to manage their data. Despite the appealing advantages of data outsourcing, cloud storage services are confronted with various threats from many aspects. Compared with traditional data storage systems (where users store their data locally), cloud storage provides users with a completely different paradigm to manage their data, which also introduces new and challenging threats towards data security. Specifically, in the cloud storage service, users do not physically own their data once outsourcing the data to a cloud server (which is subject to a cloud service provider), and these data are fully controlled by the cloud server. As such, once the cloud server (including insiders working at the cloud service provider) misbehaves, the outsourced data would suffer from threats, such as corruption, modification, removal, and privacy violation. In addition, since the data are transmitted over public and insecure networks, external adversaries (e.g., hackers) might eavesdrop on the communication channel between the user and the cloud server, tamper with the interaction messages between them, and extract the data contents from the cloud server for financial or political reasons.

This monograph gives a comprehensive overview of data security in cloud storage, which includes cloud storage reliability, cloud storage confidentiality, and data investigations in cloud storage. With these security issues, five research topics are introduced and studied, i.e., secure verification of data integrity, secure deduplication, secure keyword search, secure data provenance, and secure data time-stamping. This monograph not only presents basic paradigms and principles of the aforementioned research topics and the corresponding techniques that secure cloud storage but also provides a comprehensive survey on each of the research topics. In addition, this monograph also analyzes the relationship among these research topics.

As emerging techniques, such as indistinguishability obfuscation, blockchains, and trusted execution environments (TEEs), have been developed in the last decade, it has shown great potentials in enhancing data security. This monograph also introduces the latest advances in enhancing cloud storage reliability, confidentiality,

and investigations and analyzes their pros and cons. Finally, open research issues and future work on the related topics are also discussed.

We would like to thank Prof. Nan Cheng (Xidian University), Prof. Hongwei Li (University of Electronic Science and Technology of China), Prof. Xiaohui Liang (University of Massachusetts at Boston), Prof. Xiaodong Lin (University of Guelph), Prof. Jianbing Ni (Queen's University), Prof. Haomiao Yang (University of Electronic Science and Technology of China), Prof. Kan Yang (The University of Memphis), Prof. Shui Yu (University of Technology Sydney), Prof. Xiaojun Zhang (Southwest Petroleum University), and Prof. Jianying Zhou (Singapore University of Technology and Design) for their contributions in the presented research works. We would also like to thank Shanshan Li and Dongxiao Liu for reviewing parts of this monograph and all the members of BBCR group for the valuable discussions and their insightful suggestions, ideas, and comments. Special thanks also go to the staff at Springer Science+Business Media: Celine Chang, Susan Lagerstrom-Fife, Jane Li, and Suraj Kumar, for their help throughout the publication process.

Chengdu, China — Yuan Zhang
Chengdu, China — Chunxiang Xu
Waterloo, Canada — Xuemin Sherman Shen

Contents

Acronyms

CA	Certificate authority
CDN	Content distribution network
CE	Convergent encryption
eHealth	Electronic healthcare
EHRs	Electronic health records
EMRs	Electronic medical records
EPD	Essential provenance data
FE	Functional encryption
FHE	Fully homomorphic encryption
HIPAA	Health Insurance Portability and Accountability Act
HVTs	Homomorphic verifiable tags
IdP	Identity provider
IMEI	International Mobile Equipment Identity
$i\mathcal{O}$	Indistinguishability obfuscation
IoT	Internet of things
IRS	Index Repository Service
KGA	Keyword guessing attack
KGC	Key generation center
MHT	Merkle hash tree
MLE	Message-locked encryption
NPD	Nonessential provenance data
OPRF	Oblivious pseudorandom function
ORAM	Oblivious random access machine
PDP	Provable data possession
PIR	Private information retrieval
PKI	Public-key infrastructure
PKG	Private key generator
PoR	Proofs of retrievability
PoS	Proof of stake
PoW	Proof of work
POW	Proof of ownership

PSE	Public-key searchable encryption
SE	Searchable encryption
SSE	Symmetric-key searchable encryption
SIM	Subscriber identity module
TEEs	Trusted execution environments
TPA	Third-party auditor
TSP	Time-stamping service provider
WoL	Window of latching
WoT	Window of time-stamping