An Efficient and Secure Scheme for Dynamic Shared Data in Cloud

Zaid Alaa Hussien*
[1]Management Technical College/Basrah
Southern Technical University
Basra, Iraq
zaid.alaa@stu.edu.iq

Zaid Ameen Abduljabbar
[1]College of Education for Pure Sciences
University of Basrah
Basra, Iraq
[2]Technical Computer Engineering Department
Al-Kinoouze University College
Basra, Iraq
alsulamizaid@gmail.com

Mohammed Abdulridha Hussain
[1]College of Education for Pure Sciences
University of Basrah
Basra, Iraq
[2]Technical Computer Engineering Department
Al-Kinoouze University College
Basra, Iraq
mohsubber@gmail.com

Mustafa A. Al Sibahee
[1]Shenzhen Huazhong University of Science and Technology Research Institute
Shenzhen 518063, China
[2]Communication Engineering Department
Iraq University College
Basra, Iraq
mustafa.a@hust.edu.cn

Songfeng Lu*
[1]School of Cyber Science and Engineering
Huazhong University of Science and Technology
Wuhan, 430074, China
[2]Shenzhen Huazhong University of Science and Technology Research Institute
Shenzhen 518063, China
[3]Nanjing Souwen Information Technology Co.,Ltd
Nanjing 211800, China
lusongfeng@hust.edu.cn

Hamid A. AL-Asadi
[1]Communications Engineering Department
Iraq University College
Basra, Iraq
[2]Computer Science Department,
University of Basrah
Basra, Iraq
8655.hamid@gmail.com

ABSTRACT

People have proposed many data integrity techniques to secure data storage in cloud. The majority of these schemes assume that only the owner of the data can modify their storage in cloud. In recent years, researchers have allowed different cloud users to use integrity assurance for modifying data. As a result, schemes with stronger reality than before have been proposed. Nevertheless, these attempts are impractical due to the large computing costs for cloud users. Clients must also perform numerous computations to ensure the integrity of data storage. A robust and efficient scheme is put forward in this study to maintain data integrity in cases that involve public auditing. In this way, multiuser modification can be used to check the public integrity for cloud data and reduce the auditing cost.

The proposed scheme uses public key cryptography equipped with a proxy re-encryption and a cryptographic hash function. We allow a third-party auditor (TPA) to conduct preprocessing of data for the sake of cloud users prior to uploading these data to the cloud service providers (CSPs) and then verify the integrity of data. We also allow the TPA to perform re-encryption of data for sharing data without losing privacy. The scheme is characterised by significant security features, such as management of key, privacy, low-cost computation, exchange of key, freeing clients from burdens, failure of CSPs in creating right verifier response in absence of data and one-time key requirement. Numerical analysis and extensive experimental results verify that the proposed scheme is efficient and scalable.

CSAE 2019, October 22–24, 2019, Sanya, China

ACM ISBN 978-1-4503-6294-8/19/10$15.00
https://doi.org/10.1145/3331453.3361648

CCS CONCEPTS

• Security and privacy • Security services • Privacy-preserving protocols