2016 IEEE 2nd International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, IEEE International Conference on Intelligent Data and Security

An Efficient Public Verifiability and Data Integrity Using Multiple TPAs in Cloud Data Storage

Salah H. Abbdal[1], Hai Jin[1], Ali A. Yassin[2], Zaid Ameen Abduljabbar[1,2]
Mohammed Abdulridha Hussain[1,2], Zaid Alaa Hussien[1,3], Deqing Zou[1]
[1]Cluster and Grid Computing Laboratory
Services Computing Technology and System Laboratory
School of Computer Science and Technology
Huazhong University of Science and Technology, Wuhan, 430074, China
[2]University of Basrah, Basrah, Iraq
[3]Southern Technical University, Basrah, Iraq
manatheraa@yahoo.com, hjin@hust.edu.cn

***Abstract*—Cloud computing is a novel paradigm in information technology. This approach involves methods that forward services to users on demand via pay-as-you-go. Cloud computing can reduce computation and communication costs, and this advantage has resulted in the influx of cloud computing users. Cloud storage, which allows users to remotely outsource their data to the cloud, is considered a major cloud computing service. However, this form of storage introduces new security challenges, such as unreliable service providers. Data storage correctness is another challenge that should be addressed before this modern storage model can be extensively applied. Most proposed schemes for data integrity verification use a third party auditor, specifically a single third party auditor. However, a single third party auditor may become a bottleneck in the overall system operation and may degrade system performance because thousands of users may delegate their tasks to a single third party auditor.**

In this paper, we propose a new scheme for securing data integrity via a multiple third party auditors based mutual authentication to overcome the aforementioned limitations and ensure high-level security. We suggest a remote data storage correctness checking scheme based on homomorphic linear authentication and an elliptic curve digital signature algorithm to support public verifiability. Our proposed scheme uses a Merkle hash tree at the cloud server to store data, thereby enabling rapid data access. Finally, our proposed scheme identifies misbehaving servers and verifies data storage correctness.

***Keywords*: Cloud computing, cloud storage, data storage correctness, elliptic curve digital signature algorithm, public verifiability**

I. Introduction

Cloud computing offers users several benefits, such as high flexibility when using the cloud and the elimination of the need for expensive computing hardware and software. This approach introduces services that are highly important to users. Data storage, which allows users to outsource their data to the cloud without maintaining a local copy, is one of the key services of cloud computing [1], [2]. Cloud storage provides users the advantages of economy of scale and simultaneous reduction of the communication and computation costs of several applications [3]. However, users still encounter threats that directly affect their data, including threats to confidentiality, data integrity, and access control. Several proposed methods have attempted to address these security challenges but have insufficiently fulfilled all user requirements.

Some approaches employ a *third party auditor* (TPA) to help a user verify the data with the *cloud server provider* (CSP) because the TPA has the ability and experience that the user may not have. Furthermore, when users do not have time to perform certain operations, users delegate tasks to the TPA, who then accomplishes the tasks on their behalf. However, a *single third party auditor* (STPA) may become a bottleneck in the system and may diminish system performance [4]. Thus, we propose a new scheme that employs *multiple third party auditors* (MTPAs) to overcome these risks.

Our work also includes several security features, such as confidentiality, maintenance of privacy, and efficiency. Cloud computing has several important security challenges. A major challenge stems from data storage, which is highly significant in cloud computing. Therefore, researchers continue to search for effective ways or schemes to protect user data. Most recent studies have focused on data storage correctness [5]–[8]. Schemes that protect user data involve three entities that participate in the overall process flow (Fig. 1): (1) the cloud user, who wants to store data in the cloud; (2) the CSP, which manages and controls the data; and (3) the TPA, who verifies the data as requested by the user and may perform operational requirements for the user.

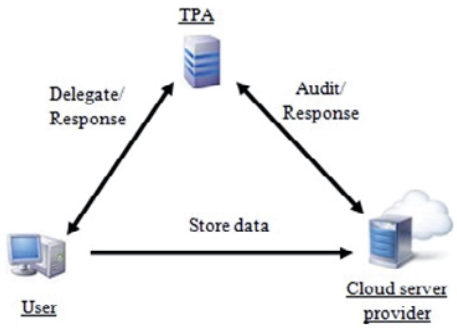

Fig. 1. Traditional Data Flow Architecture

978-1-5090-2403-2/16 $31.00 © 2016 IEEE
DOI 10.1109/BigDataSecurity-HPSC-IDS.2016.26