Chapter 46
Privacy-Preserving Public Auditing and Data Dynamics for Secure Cloud Storage Based on Exact Regenerated Code

Syam Kumar Pasupuleti
IDRBT, Hyderabad, India

ABSTRACT

Cloud storage allows users to store their data in the cloud to avoid local storage and management costs. Since the cloud is untrusted, the integrity of stored data in the cloud has become an issue. To address this problem, several public auditing schemes have been designed to verify integrity of the data in the cloud. However, these schemes have two drawbacks: public auditing may reveal sensitive data to verifier and does not address the data recovery problem efficiently. This article proposes a new privacy-preserving public auditing scheme with data dynamics to secure the data in the cloud based on an exact regenerated code. This scheme encodes the data for availability, then masks the encoded blocks with randomness for privacy of data and enables a public auditor to verify the integrity of the data. Further, this scheme also supports dynamic data updates. In addition, security and performance analysis proves that proposed scheme is provably secure and efficient.

1. INTRODUCTION

Cloud storage allows the users to store their data in cloud and access anytime from anywhere. Amazon S3 (Simple Storage Service, AWS) is an example for this. The cloud storage provides comparably lower storage cost, flexibility, location independent accessibility service to the users. Although cloud storage has these benefits, integrity of stored data in cloud has become a big concern, because cloud is untrusted and the user has no control over data after moving to cloud, i.e. data stored in the cloud can be modified, deleted, leaked, and even stolen especially in public clouds (Mather et al., 2009; Zissis et

DOI: 10.4018/978-1-7998-8954-0.ch046

al., 2010). Hence, the users require data integrity auditing mechanism along with privacy-preserving, data availability guarantee and data dynamics.

To ensure the integrity of data, several auditing schemes (Ateniese et al., 2007, 2008; Erway et al., 2009; Wang et al., 2011; Syam et al., 2012; Zhu et al., 2013) have been proposed. However, these schemes do not address the data privacy from third-party auditors i.e. the auditing processes may leak data owner's private data to external auditors. To preserve the data privacy along with integrity, the privacy-preserving public auditing schemes has been proposed (Wang et al., 2013; Hao et al., 2011; Worku et al., 2013; Yang et al., 2013; Yu et al., 2015; Wang et al., 2014). However, those schemes lacking availability of data, which is also require for data storage in the cloud addition to integrity and privacy. There are different data redundancy schemes (Jules et al., 2007; Sacham et al., 2008; Bowers et al., 2009; Cao et al., 2012; Henry et al., 2014; Kun et al., 2014) has been proposed to guaranty data availability along with integrity based on erasure codes and regenerated codes. Like integrity auditing schemes, these schemes also lacking privacy-preserving of data against the public auditor.

Recently, (Liu et al., 2015) proposed a privacy-preserving public auditing scheme for regenerated based cloud storage to achieve the integrity, availability along with privacy. Their scheme masked the encoded coefficients in the proof with the help of random bits. However, this scheme did not cover dynamic data operations. (Ren et al., 2018) proposed a dynamic proof of retrievability for cloud storage using functional regenerating codes. However, these schemes suffer from mainly two problems because of their functional repair strategy. First, these schemes not suitable for applications that are frequently access the original data. Second, due to repairing, reconstruction rules and frequently updating, it creates significant overhead whenever a failure occurs.

In this article, we propose a privacy-preserving of public auditing and data dynamics for secure cloud storage based on Exact Regenerating code (Rashmi et al., 2011). In this scheme, the data is encoded into multiple blocks and those blocks are masked with randomness. Then generates signatures for each block and uploads to cloud. Later, data integrity is verified through the challenge-response protocol. Also, this article supports dynamic data updates without retrieving data back to the user.

The main contributions of scheme as follows:

1. This scheme constructs the privacy-preserving public auditing and data dynamics for secure cloud storage based on exact regenerated code;
2. This scheme encodes data blocks and masks these blocks for data availability and privacy-preserving respectively;
3. Then, this scheme verifies integrity of data by public verifier with help of signatures and challenge-response protocol;
4. Proposed scheme also achieves dynamic data operations by using dynamic hash table;
5. This scheme proves that security and efficiency of proposed scheme in security and performance analysis.

The paper is described as follows: section 2, describes the related work, Section 3 defines the problem statement. Section 4 constructs the proposed scheme. A section 5 and 6 present's security and performance analysis respectively. Finally, conclusion of paper is given in Section 7.