
P. Syam Kumar, Pondicherry University, India
Marie Stanislas Ashok, Pondicherry University, India
R. Subramanian, Pondicherry University, India

ABSTRACT

Data storage is an important application of cloud computing, where the users can remotely store their data into the cloud. This new paradigm of data storage service also introduces security challenges, such as Confidentiality, Integrity and Availability of data. The protection of these issues in cloud is a very challenging and potentially formidable task, especially for the users with constrained resources. Therefore, an independent auditing service is required to address these issues of data stored in the cloud. The existing schemes may not scale well for this purpose. This paper proposes a publicly verifiable dynamic secret sharing scheme for the Availability, Integrity and Confidentiality of data. Their scheme takes advantages of both Secret Sharing and Tornado code which can achieve the computational security and maintain low communication overhead in terms of shortened data dispersing size. The authors’ model gives probabilistic proofs of Integrity of data by challenging random blocks from the server to reduce the computation and communication overhead, and also supports dynamic data operations to data shares in cloud using index table. Through extensive security analysis, their scheme can provide secure, dependable, and publicly verifiable cloud data storage in the Cloud against threats. Through the performance and experimental results, the authors prove that their scheme is efficient than existing schemes.

Keywords: Availability, Cloud Storage, Confidentiality, Integrity, Linear Code, Probability Detection, Secret Sharing, Tornado Code

1. INTRODUCTION

Cloud Computing is a promising computing model that enables convenient and on-demand network access to a shared pool of computing resources. Cloud computing offers a group of services including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) (Buyya, 2009). Cloud data Storage is a one of the important service of cloud computing which allows the users to move
their data from local computing systems to the cloud. More and more the users start choosing to host their data in the cloud. Because of cost effectiveness which is particularly true for small and medium-sized businesses. By moving their data to the Cloud, they can avoid the initial investment of expensive infrastructure setup, large equipments, and daily maintenance cost. They only need to pay the space they actually use, e.g., cost-per-gigabyte-stored model. Another reason is that the users can rely on the cloud to provide more reliable services, so that they can access the data from anywhere and at any time. Individuals or small-sized companies (Kan et al., 2011) usually do not have the resources to keep their servers as reliable as the Cloud does. Amazon Elastic Compute Cloud (EC2) (Amazon, 2008) and Apple Icloud (Apple Icloud, 2010) are well known examples for cloud storage. This new paradigm of data storage service also introduces security challenges related to the Confidentiality, Integrity and Availability of the data (Mather et al., 2009).

The security of data stored in the cloud is a paramount importance for their functionality. The security issues to cloud storage service are due to the following reasons (Takabi, 2010): 1) the cloud servers are exposed to untrusted environment, data may be lost due to failures of the servers. 2) The data may be stolen or modified by the unauthorized users or malicious insiders. 3) Sometimes, the cloud service provider intentionally hide data loss incidents or reclaim the storage by discarding data that has not been accessed or rarely accessed for his own benefits. 4) Although cloud infrastructures are more powerful and reliable than local devices they are subjected to the wide range of internal and external attacks. Some of the recent data loss incidents are the sidekick cloud disaster in 2009 and the breakdown of Amazon’s Elastic Computing Cloud (EC2) in 2010 are given in Cellan (2009) and Miller (2010) respectively. Hence, the efficient and effective methods are needed to ensure the Confidentiality, Integrity, and Availability of outsourced data in the cloud.

To achieve the Availability of remote data, the replication mechanisms are frequently used (Matossian, 2003). But this kind of solution has the obvious drawback of requiring a large amount of space and communication. Rabin (1989) has addressed this problem by using Information Dispersal Algorithm (IDA) but its encoding time is slow for the large files. Next, to protect the Confidentiality of data, the user encrypts the data before outsourcing. However, it is increases the responsibility of protecting the data to protect the encryption keys and brings non-trivial key management problems (Barsoum et al., 2010; Hao et al., 2010; Syam et al., 2011b). In order to protect encryption keys, the user needs to encrypt the keys again, which change the problem rather than solve it.

To ensure the data Confidentiality and elimination of key management problems for the users, (Shamir, 1979) presented a (m, n) secret sharing scheme. In this scheme, the data is partitioned into n shares and distribute to the n servers, when accessing the data at least m shares out of n should be enough to reconstruct the original data, where m<n. By doing so, no information about the original data can be leaked even if m-1 shares are compromised. However, there is one disadvantage of secrete sharing scheme that is storage inefficiency. Actually, in secret sharing scheme, each share has same size as original data. If storage space is concern, the erasure coding schemes can be used Rabin (1989). The erasure codes provide the redundancy in a more-efficient manner but it does not give perfect Confidentiality because each share may leak some information about the original data. To guarantee both the Confidentiality and Availability of data, the data can be encrypted and the encryption key can also be secret shared and distributed along with the data shares (Krawczyk, 1993a; Tu, 2010; Xiao, 2009; Ye, 2010).

Apart from the Availability and Confidentiality of data, the users also need to worry about the Integrity of their data. Data can be encrypted for a Confidentiality purpose but it does not imply Integrity, and yet user might not have a way to verify the Integrity of that data. Encryption alone is sufficient for the Confidentiality but maintaining the Integrity of data stored in
Strategic Marketing: Models and Plans
www.igi-global.com/chapter/strategic-marketing-models-plans/61888?camid=4v1a