Chapter 24
The Dynamic Data Privacy Protection Strategy Based on the CAP Theory

Xinwei Sun
Beijing Information Science & Technology University, China

Zhang Wei
Beijing Information Science & Technology University, China

ABSTRACT

With the rapid development of cloud storage technology, the cloud storage platform has gradually been used to store data. However, the privacy protection strategy provided by public cloud storage platform is hard to be trust by users. Moreover, they are unable to customize their own storage strategy according to their demands. This study proposed a consistency-availability-partition tolerance (CAP) theory -based data privacy protection strategy, which firstly employed CAP theory to provide privacy data protection for users and then offer users with choice to select corresponding privacy strategy to store data. Moreover, a total of three privacy protection strategies were put forward, focusing on the balance between data consistency and response time, data consistency and data availability, as well as response time and availability respectively.

INTRODUCTION

Cloud storage (Cloud Storage, 2015) refers to that the data of enterprises or individuals are outsourced to the third-party cloud storage service providers for storage and maintenance (Fox et al., 2009). It makes way for enterprises or individuals being free of the problems such as deficiency of local software and hardware resources, transferring inconvenience, as well as the failure and loss of storage equipment, etc. as long as paying for the needs. With the rapid development of cloud storage, more and more individuals prefer to store their own data into the public clouds by public APIs. At present, numerous famous IT enterprises worldwide have served users with highly reliable cloud storage environments that are ac-

DOI: 10.4018/978-1-5225-8176-5.ch024

cessible all the time, such as AmazonS3 (Amazon S3, 2006), Dropbox (Dropbox, 2014), Google Drive (Google Drive, 2014), OneDrive (OneDrive, 2014), and AliCloud (AliCloud, 2014), etc.

Cloud storage has many features such as cheap and easy to expand. These features will make cloud storage become a hot research when it appears. As cloud storage brings convenience to users in the continuous development, some problems in the cloud storage are gradually disclosed. When users upload private data to the cloud, they will lose absolute control over the data. Cloud storage system has an urgent security needs.

Part of users begins to be worried about the security of cloud storage. In a survey, forty percent of the Dropbox users indicate that they are most concerned about security (Cloud Storage User Survey, 2012). A survey suggested that about 80% of the enterprises were reluctant to save their internal data on the public cloud directly out of safety fears, and only 20% of users showed willingness of storing their private data on the private cloud (Twinstrata, 2012). To solve this problem, many cloud storage systems put forward corresponding security policies. The current mainstream cloud storage platforms include Amazon S3, Dropbox, iCloud, Google Drive, Microsoft OneDrive, and SugarSync (SugarSync, 2014). Further, Kuaipan (Kingsoft) and Baiduserve only the Chinese market. The mainstream primary storage systems have offered users with secure sockets layer (SSL) mechanism in the transmission process and advanced encryption standard (AES) (128-bit, 256-bit) encryption mechanism in the storage process (Amazon S3, 2006; Shraer et al., 2010; iCloud, 2013). However, it is hard for users to completely trust the safety security strategy provided by cloud storage system. Therefore, many users still encrypt their private data using local encryption methods and then upload the private data to the public cloud platform; in case of need of using, the data are firstly downloaded from the public cloud platform and then reduced using corresponding decryption methods. However, traditional encryption algorithm mainly depends on the key for encryption. Once the key is lost, the data is brought into an unsafe state.

Microsoft has proposed Cryptographic Cloud Storage in 2009 (Kamara & Lauter, 2010). Cryptographic Cloud Storage system uses encryption to protect the confidentiality of data. Cryptographic Cloud Storage system uses searchable encryption, attribute-based encryption and probable of data possession in the prototyping systems. It improves the performance of overall system while enhancing the effect of user experience.

Like the industry, academia also attaches great importance to the safety of cloud storage system. Shraer (Shraer et al., 2010) and other people proposed a trust system based on a core Set in Venus system. It through tripartite architecture to provide users with security features. In 2011, Bessani (Bessani et al., 2013) and other people proposed an idea of cloud-of-clouds in DEPSKY. To some extent alleviate the problem of data confidentiality and vendor data lock-in issues.

At present, in addition to the security, users also pay attention to the availability of the data saved in cloud. Thirty percent of Google Drive users believe that file loss is the biggest problem currently. In addition to file loss, the service suspension of the cloud storage system also bugs many users. Merely in 2013, many cloud storage systems around the world saw crashes in different degrees, such as the Google Drive, Microsoft's OneDrive, Apple's iCloud, Amazon S3. The crash of cloud storage system makes it impossible for users accessing to the data they upload to the public cloud and thus brings some economic loss to the user.

In order to solve the problem of the data security in cloud storage system and the application process. In 2011, BIAN (BIAN et al., 2011) and other people proposed a security structure of cloud storage based on dispersal. The mechanism of safety management and transmission of storage data are realized by layer through the use of information dispersal algorithms (IDA), distributed storage management,