Chapter 100
Privacy Preserving Public Auditing in Cloud: Literature Review

Thangavel M.
Thiagarajar College of Engineering, Madurai, India

Varalakshmi P.
Anna University, India

Sridhar S.
M. Kumarasamy College of Engineering, India

Sindhuja R.
Thiagarajar College of Engineering, India

ABSTRACT

Cloud computing has given a bloom to the technical world by providing various services. Data storage is the essential factor for the users who are having or working with lots and lots of data. Cloud data storage becomes the only way to store and maintain the large data, which can be accessed from anywhere and anytime. The open nature of cloud computing leads to some security issues. With respect to the cloud data storage, the Cloud Service Provider (CSP) has to provide security for the data outsourced. Data owner will be concerned on the data correctness after outsourcing into the cloud. To verify the data correctness, ensuring the state of data at the cloud data storage is needed, which is performed with the help of a Trusted Third Party Auditor (TTPA). Data owner can also perform the verification task, but it leads to computation cost and communication costs in huge amount. This survey gives a brief on public auditing schemes to explore what are all the system models designed by various researchers.

DOI: 10.4018/978-1-5225-8176-5.ch100

INTRODUCTION

Computing technologies like distributed, parallel, mobile, grid and cloud computing become essential to process huge data in an effective manner. In the recent trends, Cloud Computing is a key computing technology for everyone in the world today, because of enormous computing resources and services are available in pay per use model. Cloud computing is a technology enabling ubiquitous on demand access to a shared pool of configurable computing resources. It also has issues such as disaster recovery, abuse and nefarious use, malicious insiders, shared technology, etc. Data security issues in cloud computing are serious in many faces. Once the user outsource the data in the cloud, then the access to that data is done by any computing devices like laptop, mobile and other devices, which is allowed with a valid identity. If the data revealed by anonymous users, then in such cases sometimes even malicious insiders give the data to the competitors.

Ensuring privacy of outsourced data and the correctness of the data are considered to be a serious issue in cloud services. The availability of data is ensured by performing data duplication in different cloud servers. Maintenance of this duplicated data such as regular data updates in a dynamic form is harder to achieve. As per the researcher's statement, the privacy preservation can be achieved using appropriate cryptographic techniques. Correctness of the data at cloud storage should be ensured to provide a reliable service delivery to users. This requires data auditing through cryptographic hashing techniques. In case of data availability, replica placement leads to difficulty in achieving the dynamicity of data. Data update and maintenance is harder in this situation. So, there is a need to overcome these problems with the appropriate techniques, in order to provide a reliable, guaranteed service delivery to the cloud users and data owners.

The survey concise the methodologies followed in the existing system or technique. Identification of problems in the existing system and the performance of that system are reviewed. The auditing task performed with the help of TTPA involves challenge and response actions. This task may be handled by the data owner, but the cost required to run the system is very large.

Integrity

In general, the state of the data needs to be consistent. Once the data is outsourced from the user, it is uploaded to the server safely. The uploaded data has been modified only by the person who is authorized or owner of that data. The unnecessary modification need to be blocked. So, the integrity of the data is needed to be verified for certain time intervals.

Cloud Based Auditing

Verifying the data integrity is a major task when considering the data amount and its location. Huge amount of data in a place may lead to such violations. Periodic verification of the data will give a success to the system. It also ensures the reliable service delivery. To verify the data integrity various cryptographic mechanisms are used. If the size of the data to verify is huge, then it is hard to perform by a normal user, since normal user can have limited number of hardware resources. This situation brings a Trusted Third Party Auditor (TTPA) to perform auditing which is also called as public auditing (Figure 1). In Cloud, public auditing is done by the TTPA where he initially gets the request from the Data Owner or the Client to perform auditing for the specific file or blocks of a file. He also receives the metadata to compute a