Cloud Data Auditing Techniques with a Focus on Privacy and Security

ABSTRACT

Storing large amounts of data with cloud service providers (CSPs) raises concerns about data protection. Data integrity and privacy can be lost because of the physical movement of data from one place to another by the cloud administrator, malware, dishonest cloud providers, or other malicious users who might distort the data. Hence, saved data corrections must be varied at regular intervals.

EXISTING SYSTEM

Nowadays, with the help of cryptography, verification of remote (cloud) data is performed by third-party auditors (TPAs). TPAs are also appropriate for public auditing, oaring auditing services with more powerful computational and communication abilities than regular users. In public auditing, a TPA is designated to check the correctness of cloud data without retrieving the entire dataset from the CSP. However, most auditing schemes don't protect user data from TPAs; hence, the integrity and privacy of user data are lost. Our research focuses on cryptographic algorithms for cloud data auditing and the integrity and privacy issues that these algorithms face. Many approaches have been proposed in the literature to protect integrity and privacy; they're generally classified according to data's various states: static, dynamic, multiowner, multiuser, and so on.

Disadvantages

- It can't provide data privacy because the TPA doesn't retrieve data using a data generator key algorithm.
- new privacy-preserving protocols are critical for maintaining data integrity and privacy.

PROPOSED SYSTEM

CSPs usually provide clients with dynamic resource allocation such that the CSP doesn't over- or under provide resources. Numerous CSPs are commercially available; thus, the first questions clients should ask before opting for CSP services (such as information as a service, platform as a service, and software as a service) are whether the CSP provides elasticity of services, will meet the agreed service level of the agreement, and has the required architecture to run the desired services. An architecture for auditing should also be provided, where all the modules responsible for the auditing process are programmed and assigned a duty for their role in the process.

Advantages

- Randomization of data blocks and tags is the most suitable technique for preventing data leakage during auditing's proofing phase.
- To gain the faith of cloud users, CSPs must have flexible services.

SOFTWARE REQUIREMENTS

Front-end	:	JSP
Back-End	:	MySQL
Server	:	Tomcat Server
OS	:	WINDOWS 7/above

HARDWARE REQUIREMENTS

PROCESSOR	:	CORE i3
RAM	:	512MB-2GB
HARD DISK	:	40GB