**Dynamic and Public Auditing with Fair Arbitration for Cloud Data**

**ABSTRACT:**

Cloud users no longer physically possess their data, so how to ensure the integrity of their outsourced data becomes a challenging task. Recently proposed schemes such as “provable data possession” and “proofs of retrievability” are designed to address this problem, but they are designed to audit static archive data and therefore lack of data dynamics support. Moreover, threat models in these schemes usually assume an honest data owner and focus on detecting a dishonest cloud service provider despite the fact that clients may also misbehave. This paper proposes a public auditing scheme with data dynamics support and fairness arbitration of potential disputes. In particular, we design an index switcher to eliminate the limitation of index usage in tag computation in current schemes and achieve efficient handling of data dynamics. To address the fairness problem so that no party can misbehave without being detected, we further extend existing threat models and adopt signature exchange idea to design fair arbitration protocols, so that any possible dispute can be fairly settled. The security analysis shows our scheme is provably secure, and the performance evaluation demonstrates the overhead of data dynamics and dispute arbitration are reasonable.

**EXISTING SYSTEM:**

* First of all, earlier auditing schemes usually require the CSP to generate a deterministic proof by accessing the whole data file to perform integrity check.
* Secondly, some auditing schemes provide private verifiability that require only the data owner who has the private key to perform the auditing task, which may potentially overburden the owner due to its limited computation capability.
* Thirdly, PDP and PoR intend to audit static data that are seldom updated, so these schemes do not provide data dynamics support. But from a general perspective, data update is a very common requirement for cloud applications.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Providing data dynamics support is the most challenging. This is because most existing auditing schemes intend to embed a block’s index *i* into its tag computation, which serves to authenticate challenged blocks. However, if we insert or delete a block, block indices of all subsequent blocks will change, then tags of these blocks have to be re-computed. This is unacceptable because of its high computation overhead.
* Current research usually assumes an honest data owner in their security models, which has an inborn inclination toward cloud users. However, the fact is, not only the cloud, but also cloud users, have the motive to engage in deceitful behaviors.
* In Existing System no integrity auditing scheme with public verifiability, efficient data dynamics and fair disputes arbitration.
* Existing system has the limitation of index usage in tag computation
* In Existing System tag re-computation caused by block update operations
* In Existing System both clients and the CSP potentially may misbehave during auditing and data update

**PROPOSED SYSTEM:**

* We address this problem by differentiating between tag index (used for tag computation) and block index (indicate block position), and rely an index switcher to keep a mapping between them. Upon each update operation, we allocate a new tag index for the operating block and update the mapping between tag indices and block indices. Such a layer of indirection between block indices and tag indices enforces block authentication and avoids tag re-computation of blocks after the operation position simultaneously. As a result, the efficiency of handling data dynamics is greatly enhanced.
* Furthermore and important, in a public auditing scenario, a data owner always delegates his auditing tasks to a TPA who is trusted by the owner but not necessarily by the cloud.
* Our work also adopts the idea of signature exchange to ensure the metadata correctness and protocol fairness, and we concentrate on combining efficient data dynamics support and fair dispute arbitration into a single auditing scheme.
* To address the fairness problem in auditing, we introduce a third-party arbitrator(TPAR) into our threat model, which is a professional institute for conflicts arbitration and is trusted and payed by both data owners and the CSP. Since a TPA can be viewed as a delegator of the data owner and is not necessarily trusted by the CSP, we differentiate between the roles of auditor and arbitrator. Moreover, we adopt the idea of signature exchange to ensure metadata correctness and provide dispute arbitration, where any conflict about auditing or data update can be fairly arbitrated.
* Generally, this paper proposes a new auditing scheme to address the problems of data dynamics support, public verifiability and dispute arbitration simultaneously.

**ADVANTAGES OF PROPOSED SYSTEM:**

* The proposed system solves the data dynamics problem in auditing by introducing an index switcher to keep a mapping between block indices and tag indices, and eliminate the passive effect of block indices in tag computation without incurring much overhead.
* The proposed system extend the threat model in current research to provide dispute arbitration, which is of great significance and practicality for cloud data auditing, since most existing schemes generally assume an honest data owner in their threat models.
* The proposed system provides fairness guarantee and dispute arbitration in our scheme, which ensures that both the data owner and the cloud cannot misbehave in the auditing process or else it is easy for a third-party arbitrator to find out the cheating party.

**SYSTEM ARCHITECTURE:**



**MODULES**

* Data User Module.
* Third Party Auditor(TPA) Module
* Third Party Arbitrator(TPA) Module
* Cloud Module

**MODULES DESCRIPTION**

**Client Module**

* This module includes the User registration and user login details.
* Every User need to register while accessing to the cloud.
* Every User will be activated by the Cloud.
* After Cloud activated, every Client need to provide public key to login the user home.
* Public key will be provided by third party auditor.
* Client can view file details and can insert, modify and delete the file with help of TPAR.
* Client will have the TPAR message whenever the user update the file.

**Third Party Auditor (TPA) Module**

* It acts as semi-cloud.
* TPA Provide public key for every user to access the user home page.
* After cloud given auditing proof then only TPA can audit all files.

**Third Party Arbitrator (TPA) Module**

* It acts as fair dispute for users and cloud.
* Intimate the files message, each time user insert, modify, delete files to cloud.
* Send TPAR message to user and cloud.

**Cloud Module**

* Activate data client.
* Cloud sends storage auditing proof for all files to TPA.
* Cloud can view the client downloaded files from cloud.
* Cloud will have the TPAR message whenever the user updates the file.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1GB.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 7.
* Coding Language : JAVA/J2EE
* Tool : Netbeans 7.2.1
* Database : MYSQL

**REFERENCE:**

Hao Jin, Hong Jiang, *Senior Member, IEEE,* and Ke Zhou, “Dynamic and Public Auditing with Fair Arbitration for Cloud Data”, **IEEE TRANSACTIONS ON CLOUD COMPUTING 2016.**