Proving Cloud Storage Data Integrity

Treating data as a matrix allows for a novel approach to providing an audit process to a client storing data on a Cloud provider. Trading minimized persistent storage for linear computation in this Proof of Retrievability scheme leads to considerable financial benefit to the client.

Problem Statement and Goals

A Cloud storage service may either accidentally delete or maliciously corrupt a user’s data without their knowledge. How can the user efficiently check the complete integrity of their remotely-stored data?

An audit protocol can verify data integrity:

- Client challenges Cloud server randomly
- Cloud server proves to the client by computing a response
- Client verifies through computation with stored values

Approach

Results

- Confirmed linear scaling of server audit computation
- Justified choice of linear time audit protocol
- Measured vastly decreased persistent storage
- This audit protocol, run every three hours, is still more financially favorable to a PoR scheme with just 2x storage overhead.
- Parallelizing over multiple VMs to decrease audit time is underway
- Changing matrix dimensions is planned

Michael Hanling
United States Naval Academy