Cloud data auditing

It is the process of monitoring and tracking data access, usage and modifications in cloud storage.

ex - Google cloud storage have data auditing method to store the track of files activity. such as view, edit, download.

It ensures compilance, security and accountability.

It helps to detect unauthorized access.

(During audit)

In data auditing, to verify the data,

1. Query : ask the database for a report of who accessed the customer data & when
2. Proof : report shows names of employee who accessed the data & the time.
3. validation: they check the report against employee records and verify it.

(Q, P, V)

↳ ~~doing~~

Static data and dynamic data

- Static data refers to information that remains unchanged, eg - company policies (read only)
- dynamic data - data that changes freaquently ~~or~~. where data can be delete, update & modified. (read & write only)
  eg - stock price.

these types of data used in cloud.

Proof of Storage are the ~~data~~ cloud data auditing method which ensure the data integrity.

In auditing,

- before uploading data on cloud, client set the authenticator tag with each data and then upload it.

during audit,

client download ~~it and checks the~~ entire file along with its authenticator, and verifies that the authenticator same or not

- authenticator uses cryptographic algo (~~RSA~~ hashing collision ~~resistent~~ resistent)

Proof of storage

- It is a cryptographic protocol used to verify that a storage service provider is storing data as claimed.
- It ensures data integrity and provides assurance to data owners that their data is being stored securely & reliably.

It is needed,

1. verification: It allows owner to verify their data is being stored correctly or not.
2. Data Integrity - data owners ensure that their data has not been altered.

3. TYPE OF POS Scheme → next page
- It uses SHA-256 for authentication

POS Scheme protocols

1. Init : It establish a connection between a client & a storage provider.
   - with generating keys & other parameters. (~~[illegible]~~)
2. Read & write : It allows the client can access, upload & modify the data.
3. Audit : this protocol allows the client can verify its data is that is stored securely or not.

- here service level agreement is used to make connections.

data can be verify in two ways -
public verification and private verification

- public verification - anyone can verify the integrity of stored data without access to the original data.
  this verification enhance transparency.
  eg - proof is present in the form of cryptographic proof of storage of any client data.
  (uses - digital signature)

- Private verification - only authorized parties can access the original data and can verify its integrity.
  (uses - Pseudo Random fn, MAC)

In Public verification scheme, Third party auditor (TPA) used to verify the public data without getting sensitive inform—

→ To verify data, the client needs to download it and then verify it, It consume so much time and memory. (computation cost)

→ Instead verifying entire data, data is verifying into blocks.

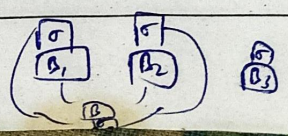
• Blockless verification

It is a technique to verify the integrity of stored data without processing entire data.

- Query send as a blocks and only that blocks download it and then verify it.

• Several blocks in one blocks • several σ in one σ.

Proof size = O(1)
validation size = O(1)



Type of Proof of storage-

1. Provable Data possession (PDP)
2. Proof of Retrievability (POR)

→ go to the next page

PDP :- (Provable data possession)

- The client uploads their data to the server along with authentication tags for each data block.
- During audits, the client checks only a sample of blocks to verify integrity.
- PDP may miss detecting corruption in individual blocks if they are not audited.

PoR :- (Proof of retrieval)

- addressing the limitations of PDP
- The clients uploads the data file, which encoded with error correcting codes along with authentication tags for each encoded data blocks.
- During audits, the client verifies the entire data files integrity.
- POR ensures that if the server passes the audit, it guarantees the retrievability of every single block.
  - client can access each data block and ensures that each are safe, from server (and not tampered)

note (audit passes means verification process is successful)

- error correcting code are Reed-Solomon code.
- From error correcting code, it can reconstruct the missing block from its parity blocks, if any block is missed/corrupt
  - if reconstruction is successful then retrieved block is for verification check, then audit passes.

performance of proof of storage scheme based on these parameters

1. Client-side storage - amount of storage required on client side to implement the scheme (POR, PDP)
2. Server " " - ——— ——— server side
3. client " computation - computation cost required during initiation, reading, writing & auditing processes on client side
4. Server " " - ——— ——— server side
5. client server communication ~~bandwidth~~ =

The amount of data transferred between the client & server during during ~~same~~ init, reading, writing & auditing process of task.

Security protocol of POS :-

1. Authenticity - It ensures that data retrieved from the storage provider is genuine & originated from the client. It involves verifying the origin & integrity of the data to prevent unauthorized modifications.
2. Freshness - It ensures that the data retrieved from the ~~Server~~ storage is up to date and has not been tempered with since it was last stored.
3. Retrievability - It ensures that the storage providers can retrieve and provide access to the stored data upon request from client.