Instant Auditing of Cloud Storage Access without Accumulating Attestations

Advicer : Gwan-Hwan Hwang
Student : Wei-Chih Chien

NTNU CSIE CCLAB

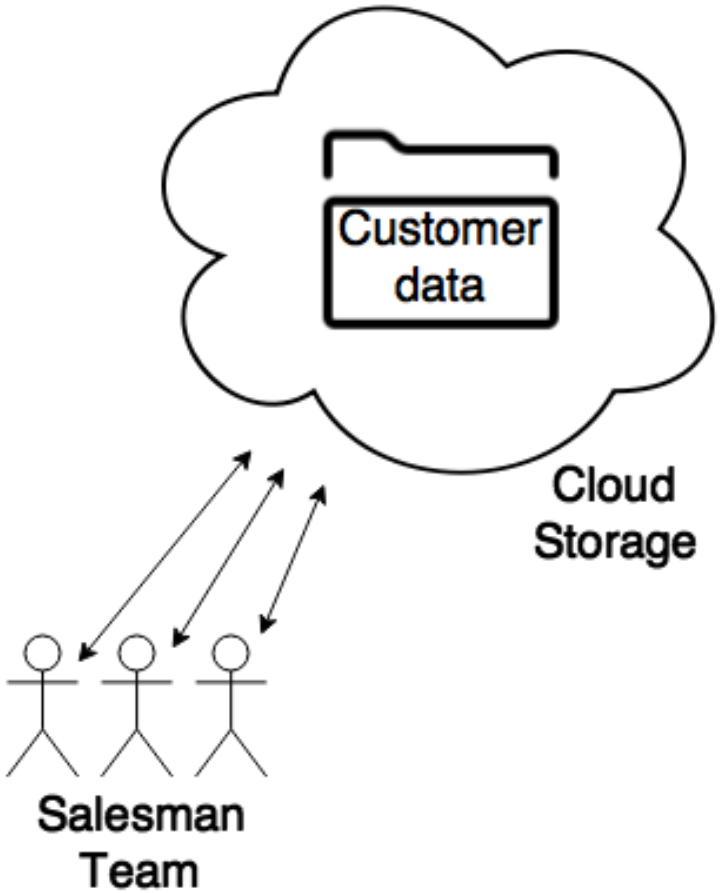
2015.10.29

Outline

Outline

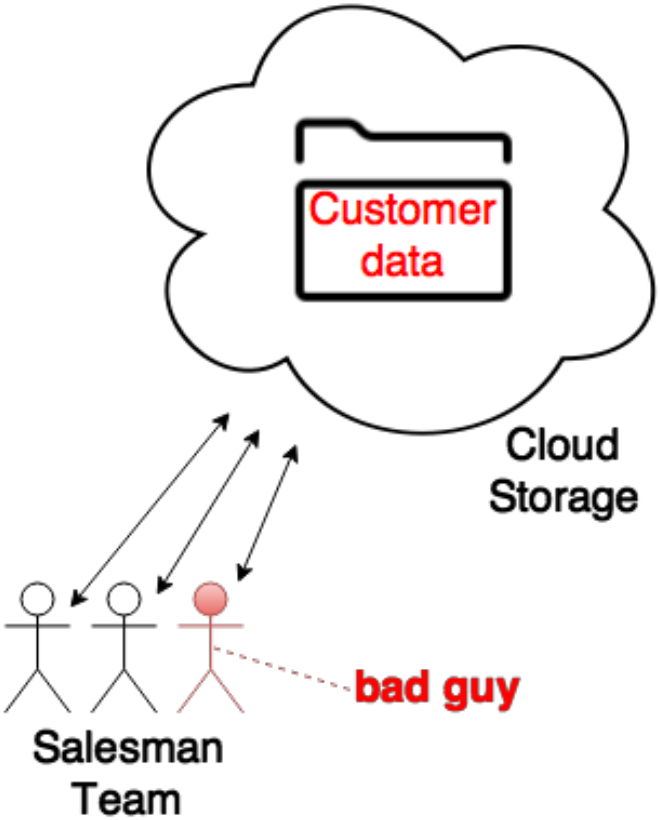
Scenario

Why Real-time Auditing?



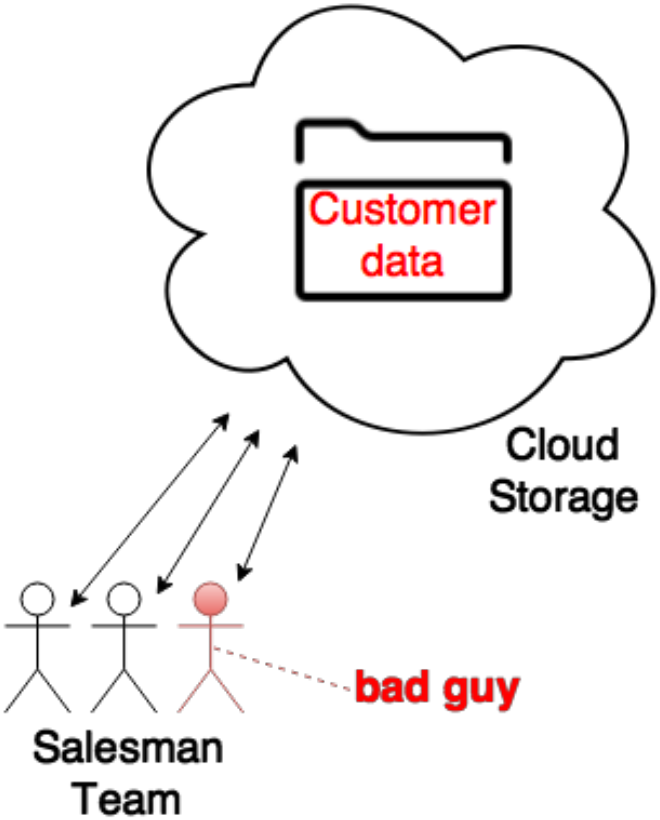
Scenario (CON'T)

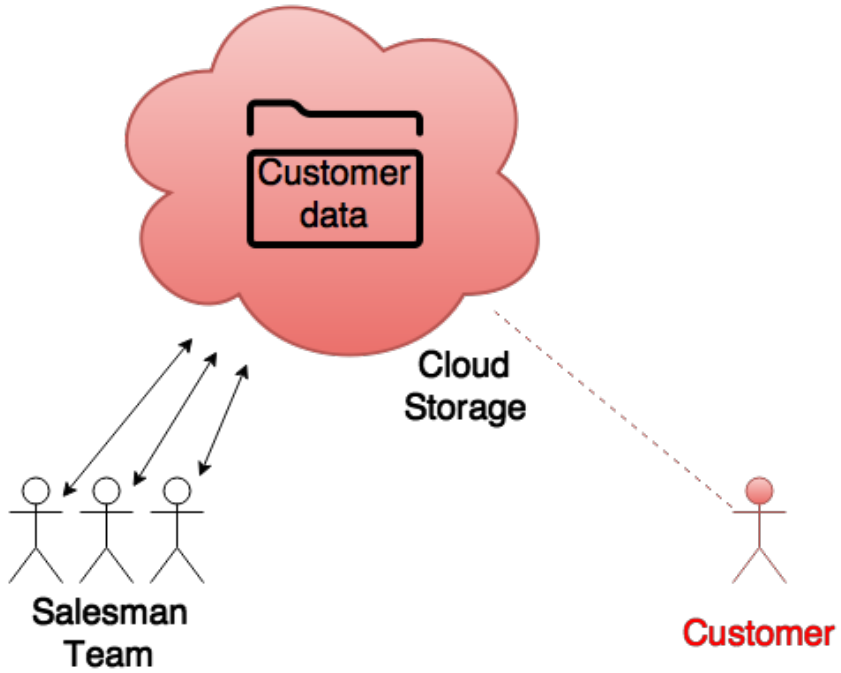
Problems



Scenario (CON'T)

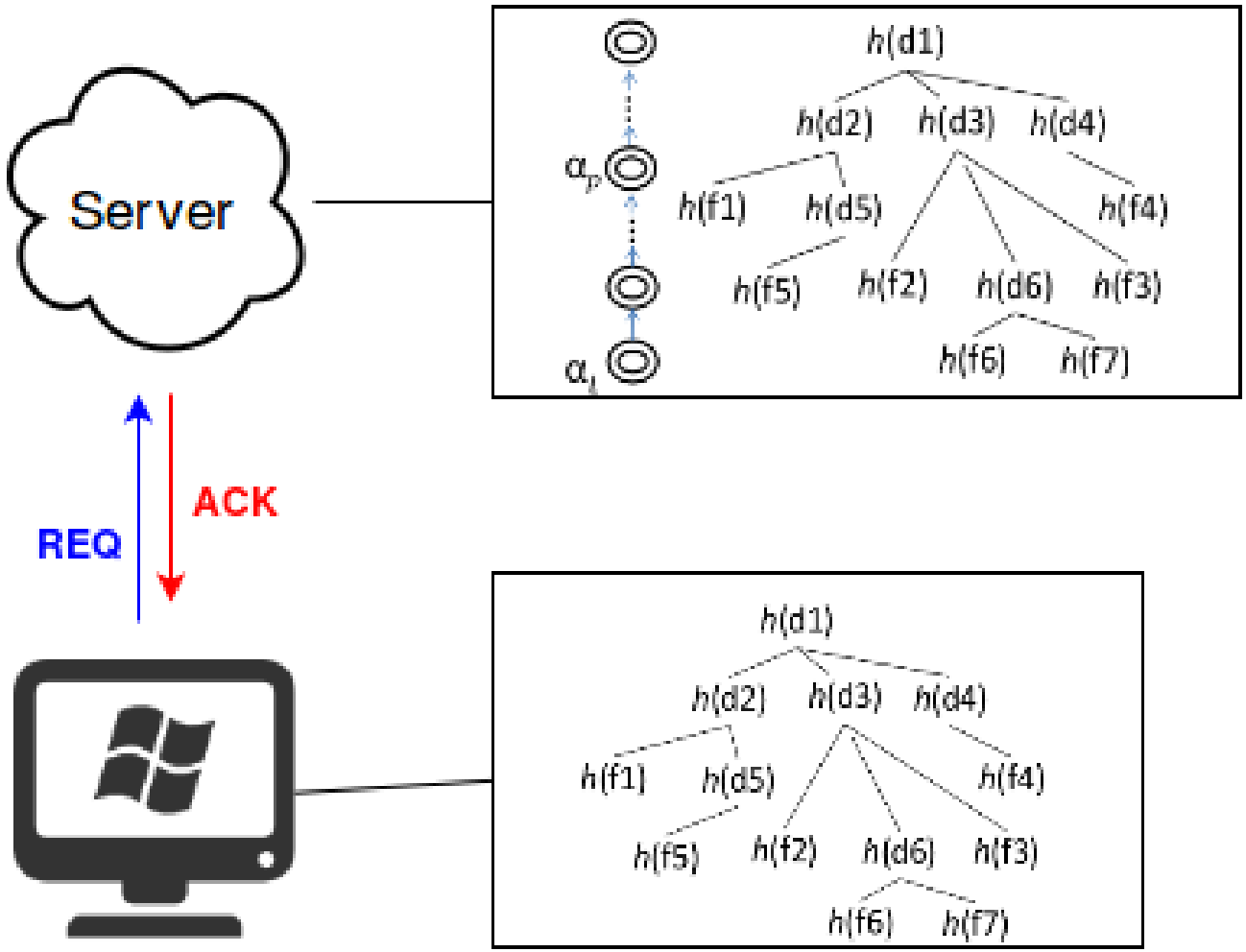
Problems

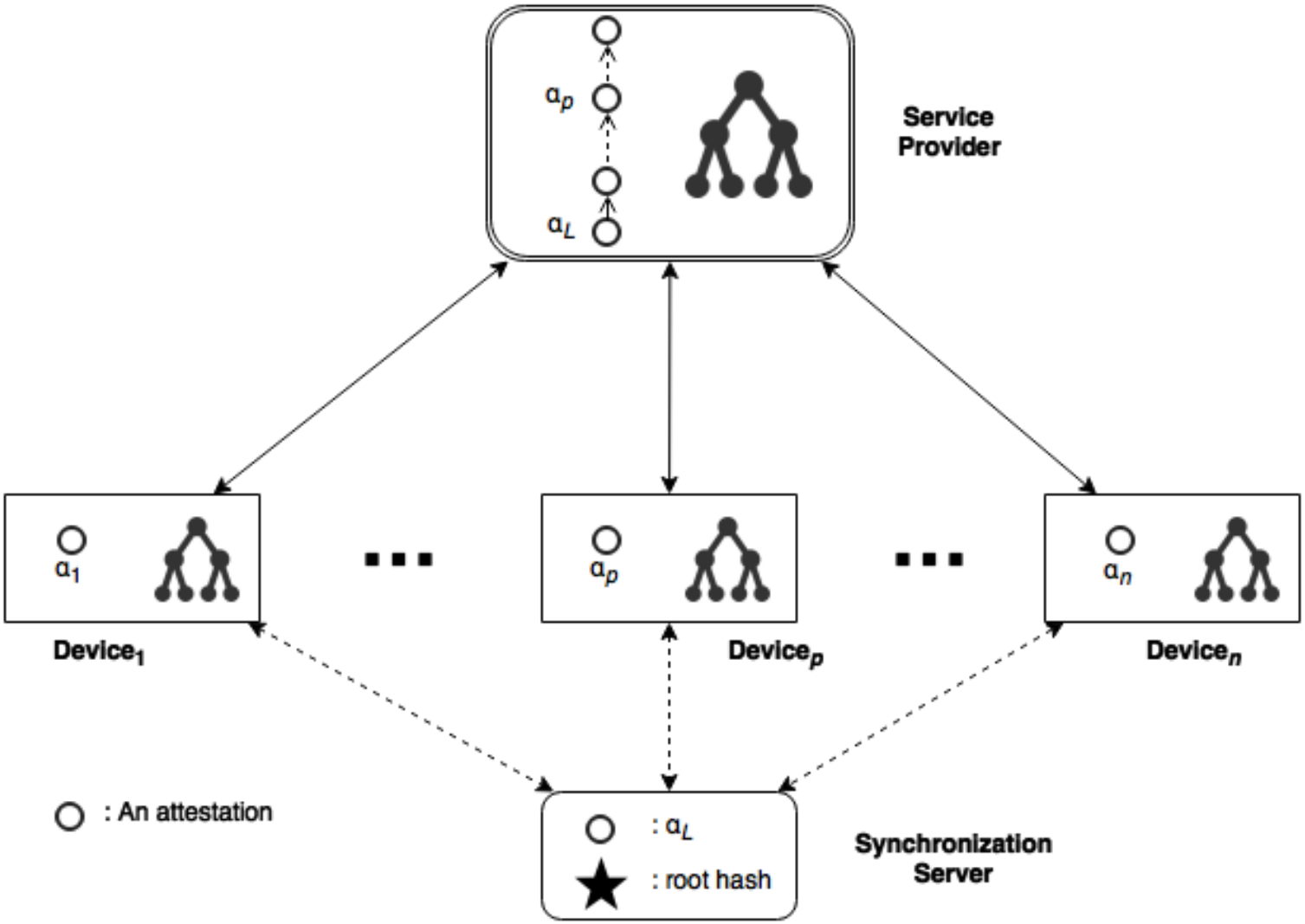




Outline

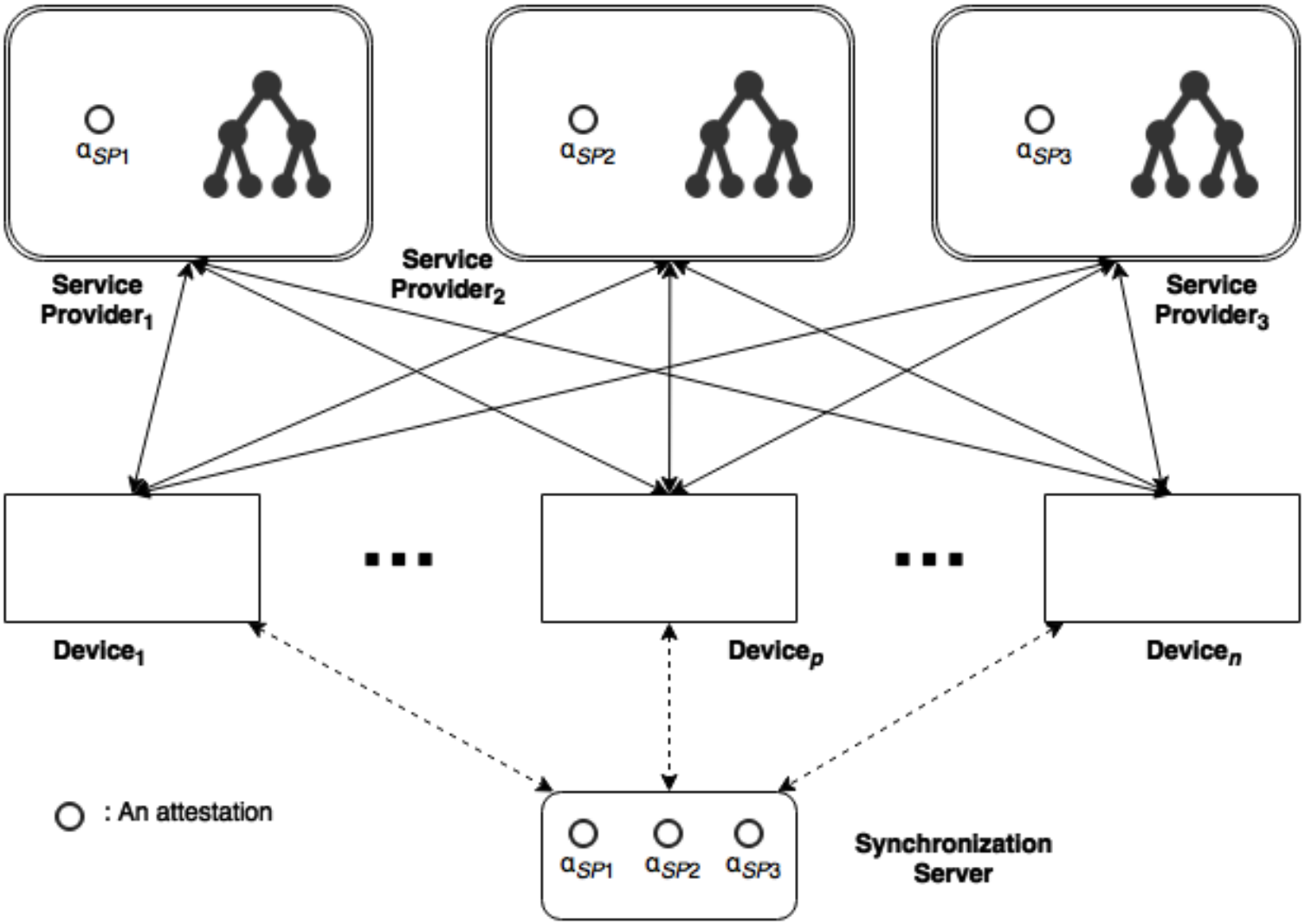
Intuitive Method





Worst-case : 累積大量未更新的動作造成系統緩慢

My Method



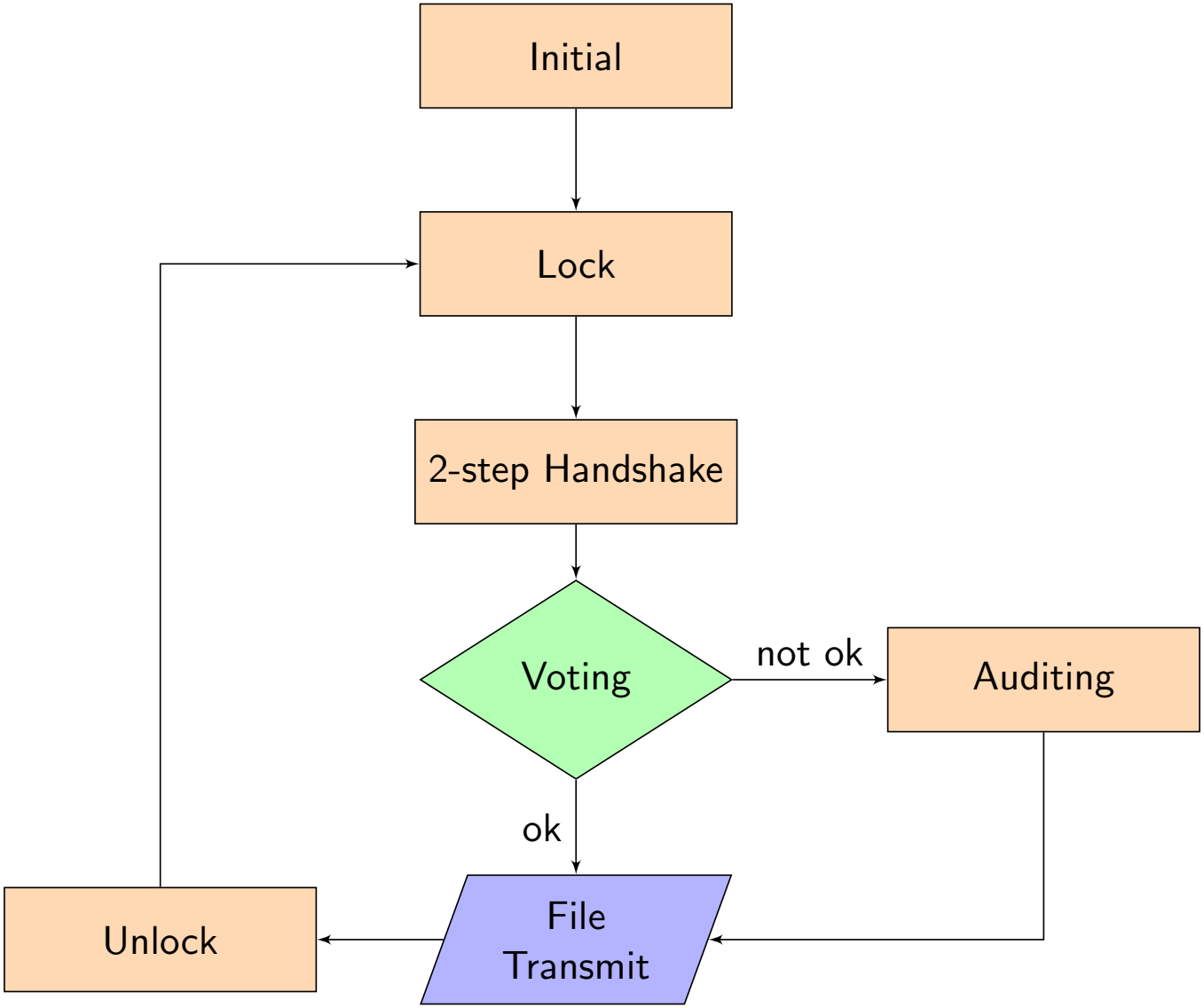
Assumption: 同時有k個server上同一file出問題的機率 ≈ 0

Comparison

- Pros
  1. Service Provider 不用累積證據
  2. Client 不用佔用空間儲存證據
  3. 資料有多份備份
  4. 花費較少的時間更新到最新的狀態
- Cons
  1. 硬體成本較高
  2. 需要處理多份 Response

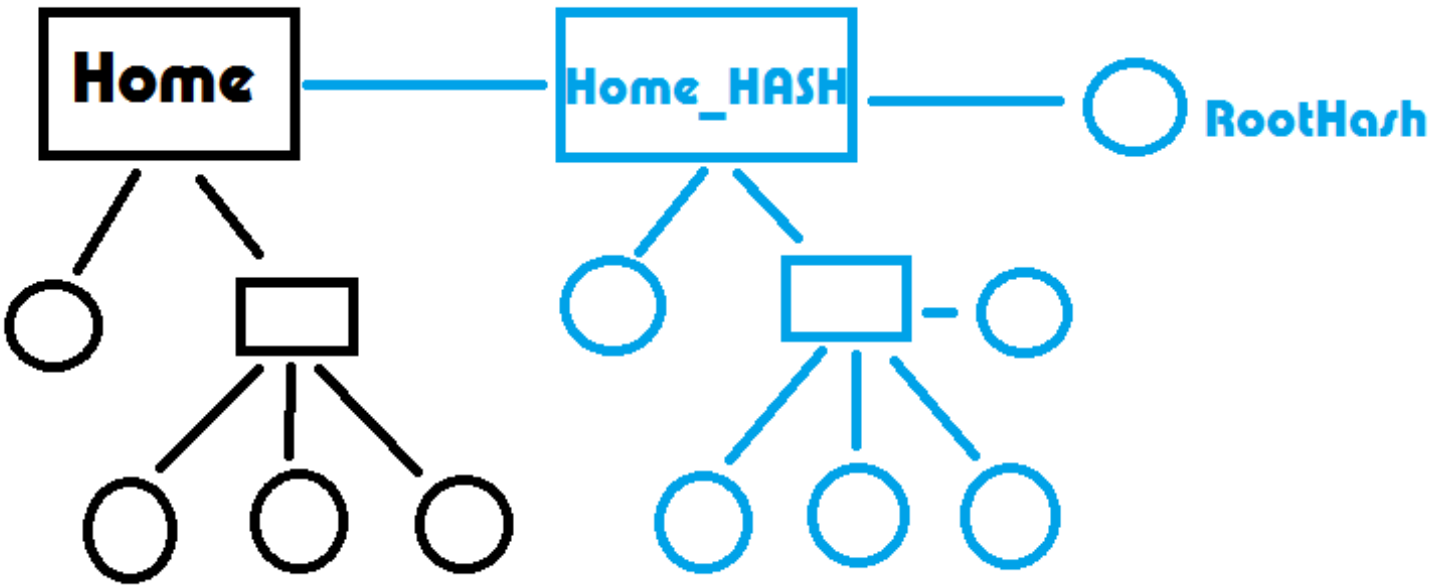
Outline

Flowchart


Initial
Lock
2-step Handshake
Voting
not ok
Auditing
ok
File
Transmit
Unlock

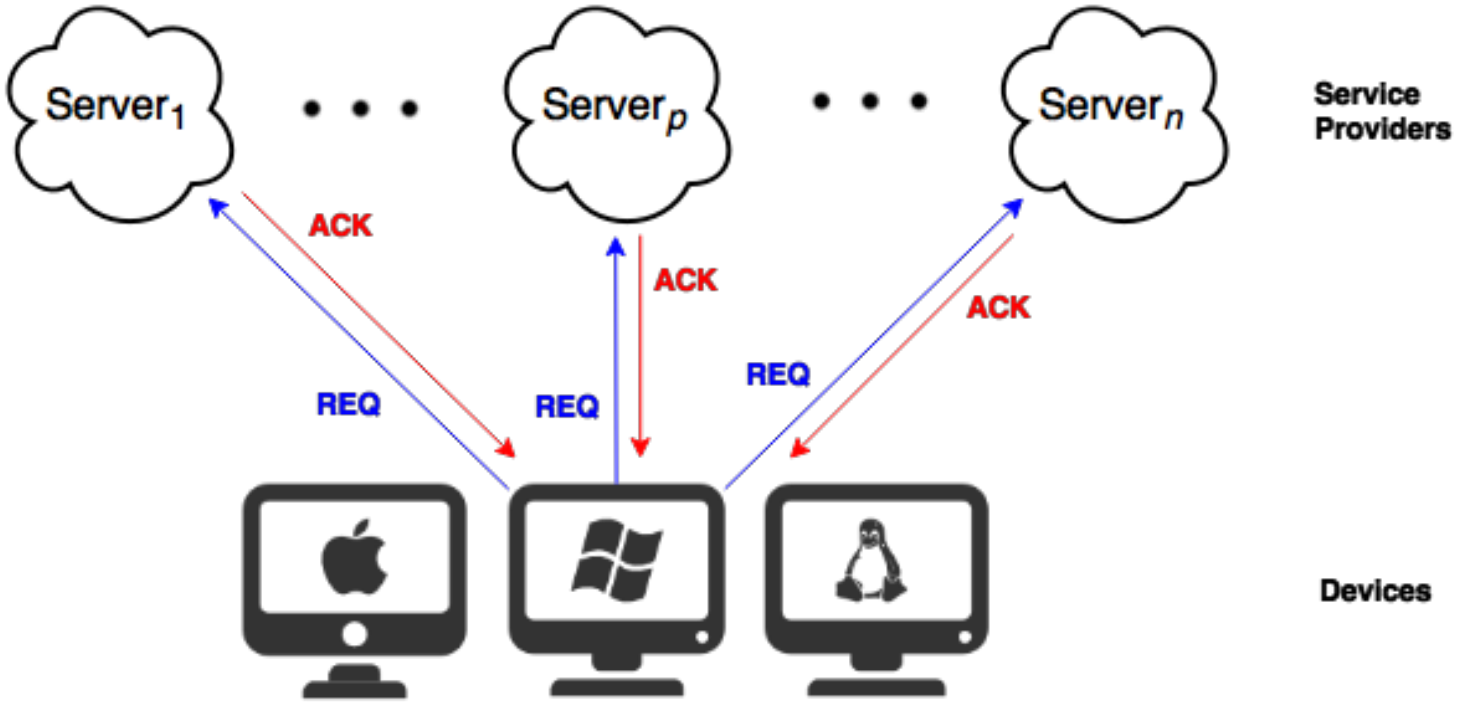
Initial

File → Merkle Tree



READ

I. 2-step Handshake & Voting

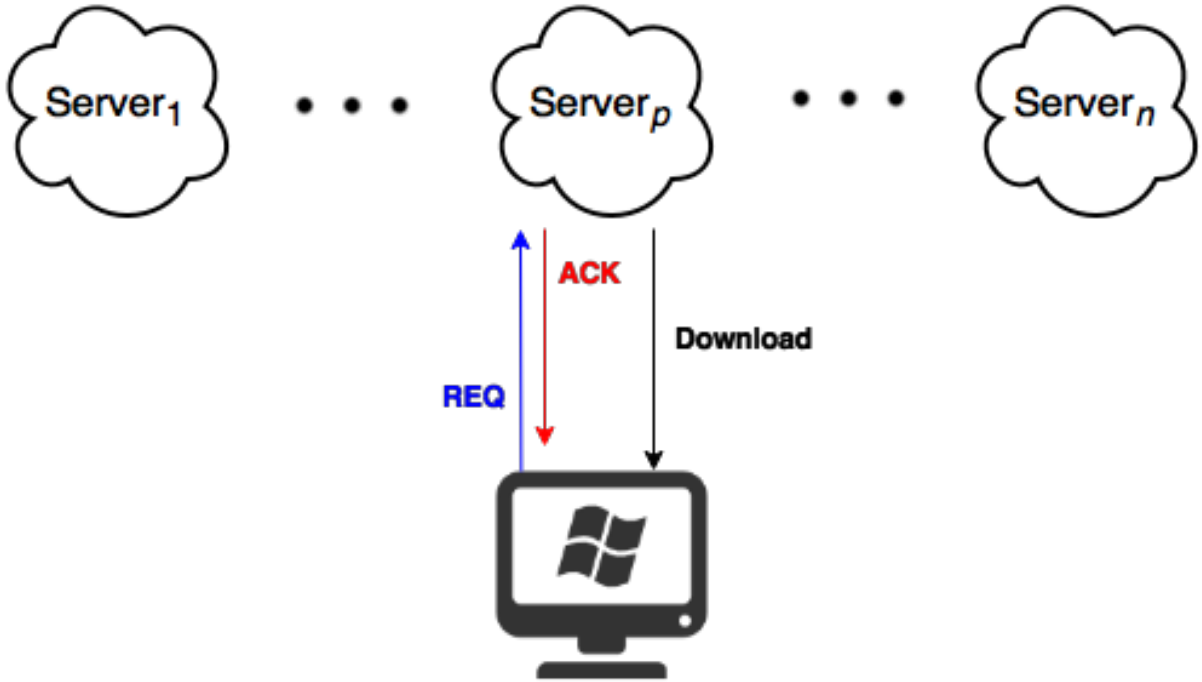


$$REQ = (op, [op]_{pri(D)})$$

$$ACK = (result, REQ, [result, REQ]_{pri(S)})$$

READ

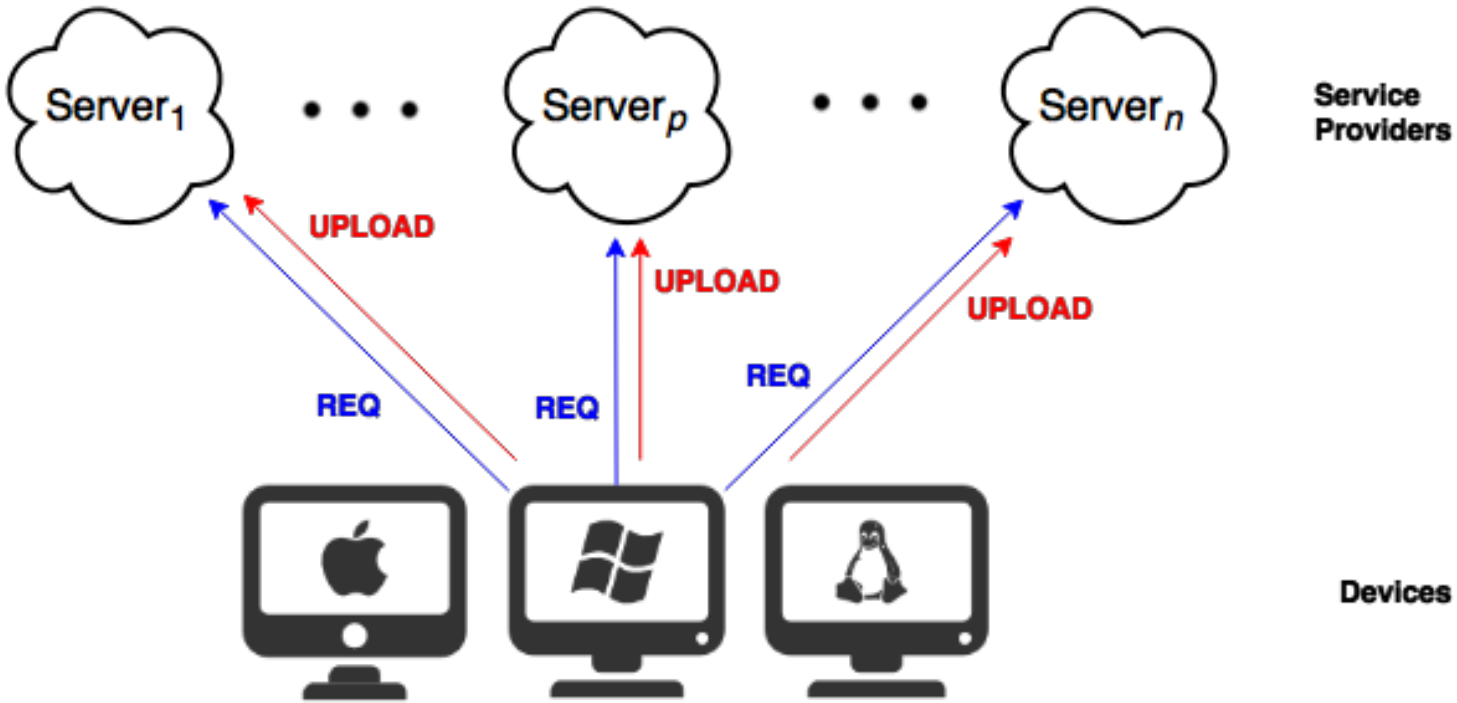
II. Download



$$\mathbf{REQ} = (\mathbf{op}, [\mathbf{op}]_{\mathbf{pri(D)}})$$
$$\mathbf{ACK} = (\mathbf{result}, \mathbf{REQ}, [\mathbf{result}, \mathbf{REQ}]_{\mathbf{pri(S)}})$$

WRITE

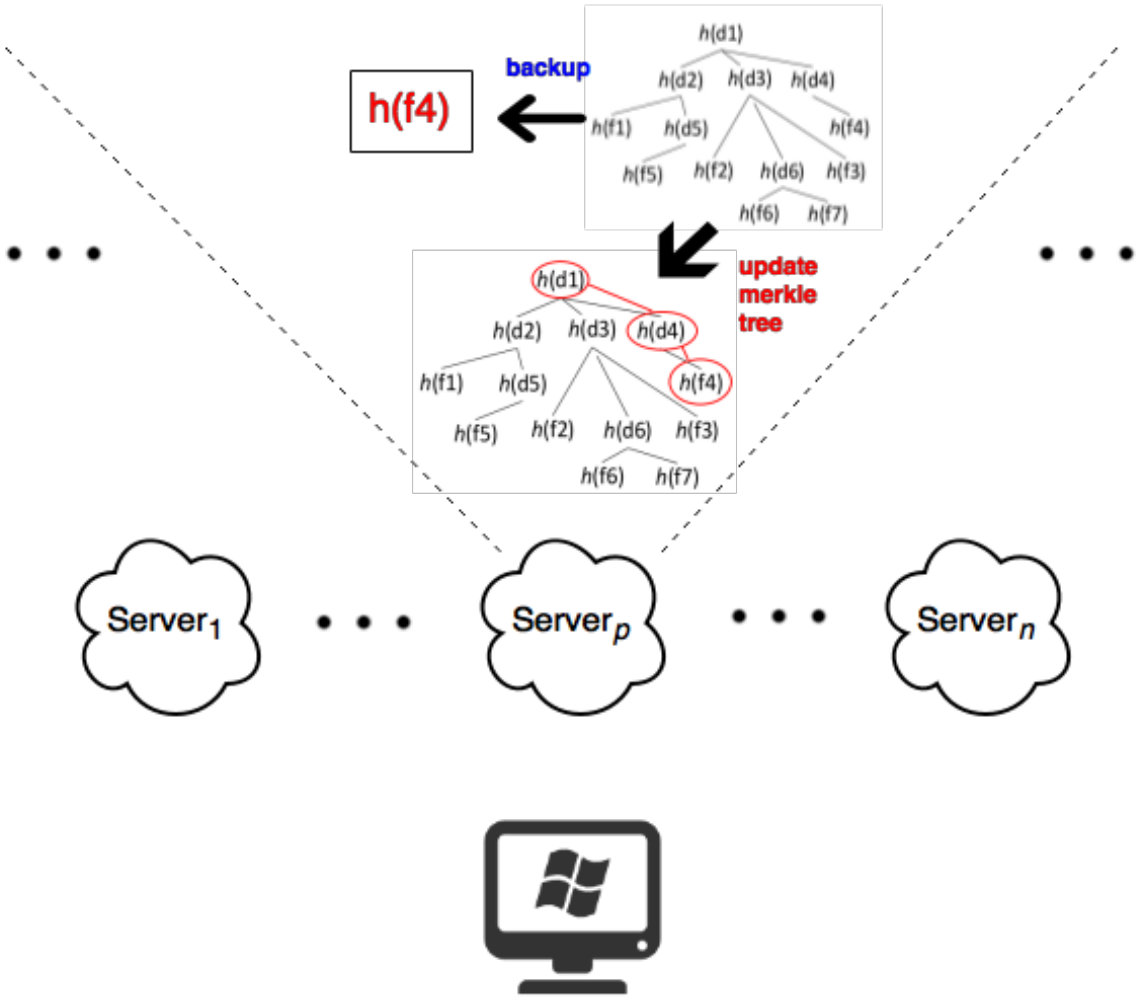
I. Upload



$$REQ = (op, [op]_{pri(D)})$$

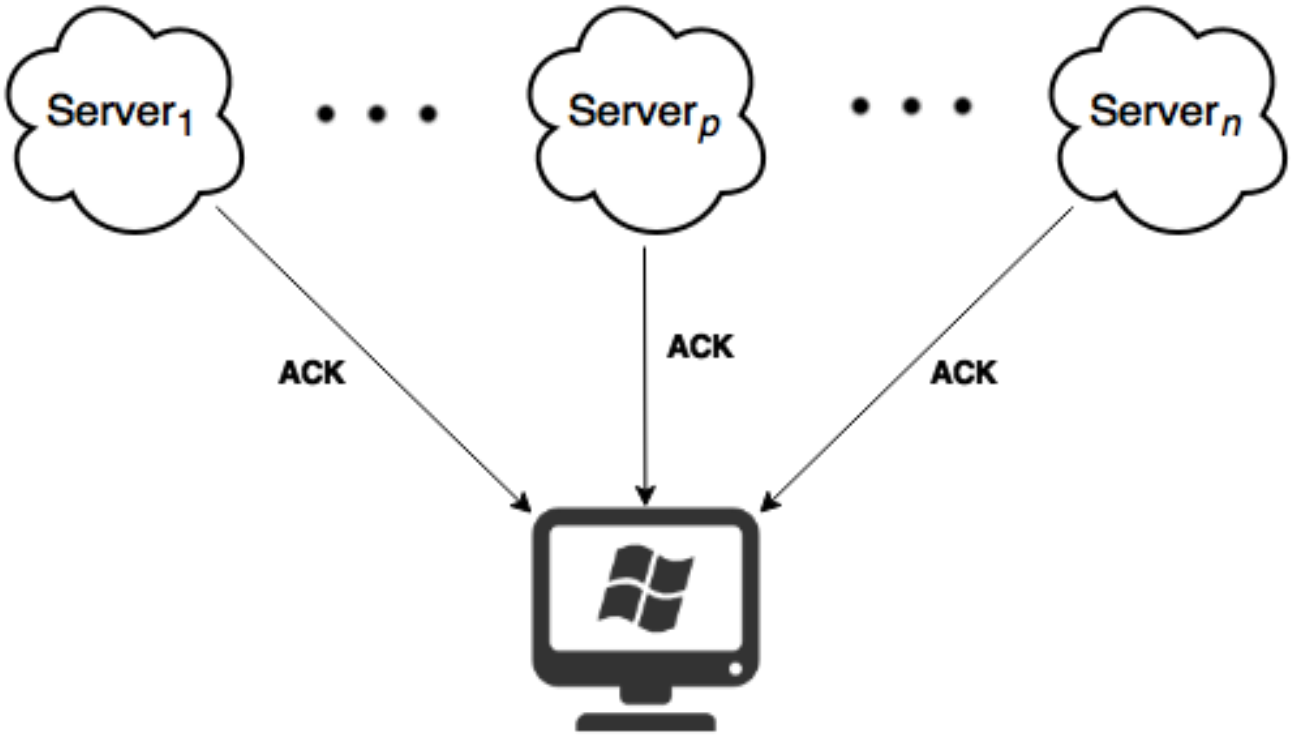
WRITE

II. Update Merkle Tree



WRITE

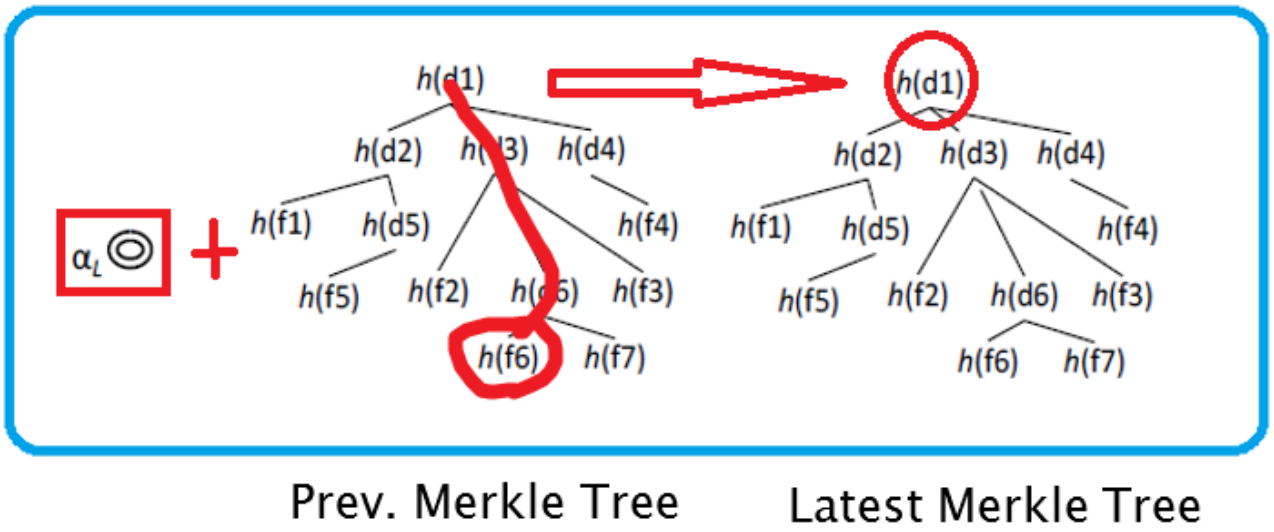
III. Voting



$$ACK = (result, REQ, [result, REQ]_{pri(S)})$$

AUDIT

1. Device 向 Synchronization Server 取得 Latest Ack.
2. Device 再向 Service Provider 取得 前一版本的 Merkle Tree.
3. 使用 Step I. 的 Ack 包含的檔案 Hash 值
   來更新 Step II. 的 Merkle Tree.



4. 比較 Device 自己算出的 Roothash 值是否和 Server 提供的相同.

Outline

Create Merkle Tree

Account A 666 MB 42 files 6 directories

Table : THE EXECUTION TIME OF FOLLOWING OPERATIONS (IN MS)

Operations	Senior	My
Request 100 times DOWNLOAD	*6332*	*6609*
Request 100 times UPLOAD	*4271*	*3054*
Audit after Download	*48*	*12*
Audit after Upload	*46*	*5*

Test File : 1644 byte

Outline

Schedules

1. My Method Finished.
   - Merkle Tree Implements.
   - Operation Handle (Read, Write and Audit).
   - File Transmit.
   - Object Transmit (Serialization).
   - Synchronization Server Implements.
2. Wei-Shian's Method Finished.
   - Attestation Chain Implements.
3. Network Problems.
4. VM Problems.
5. Design Different Experiments.

Thank You!