Instant Auditing of Cloud Storage Access without Evidence Cached

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

NTNU CSIE CCLAB

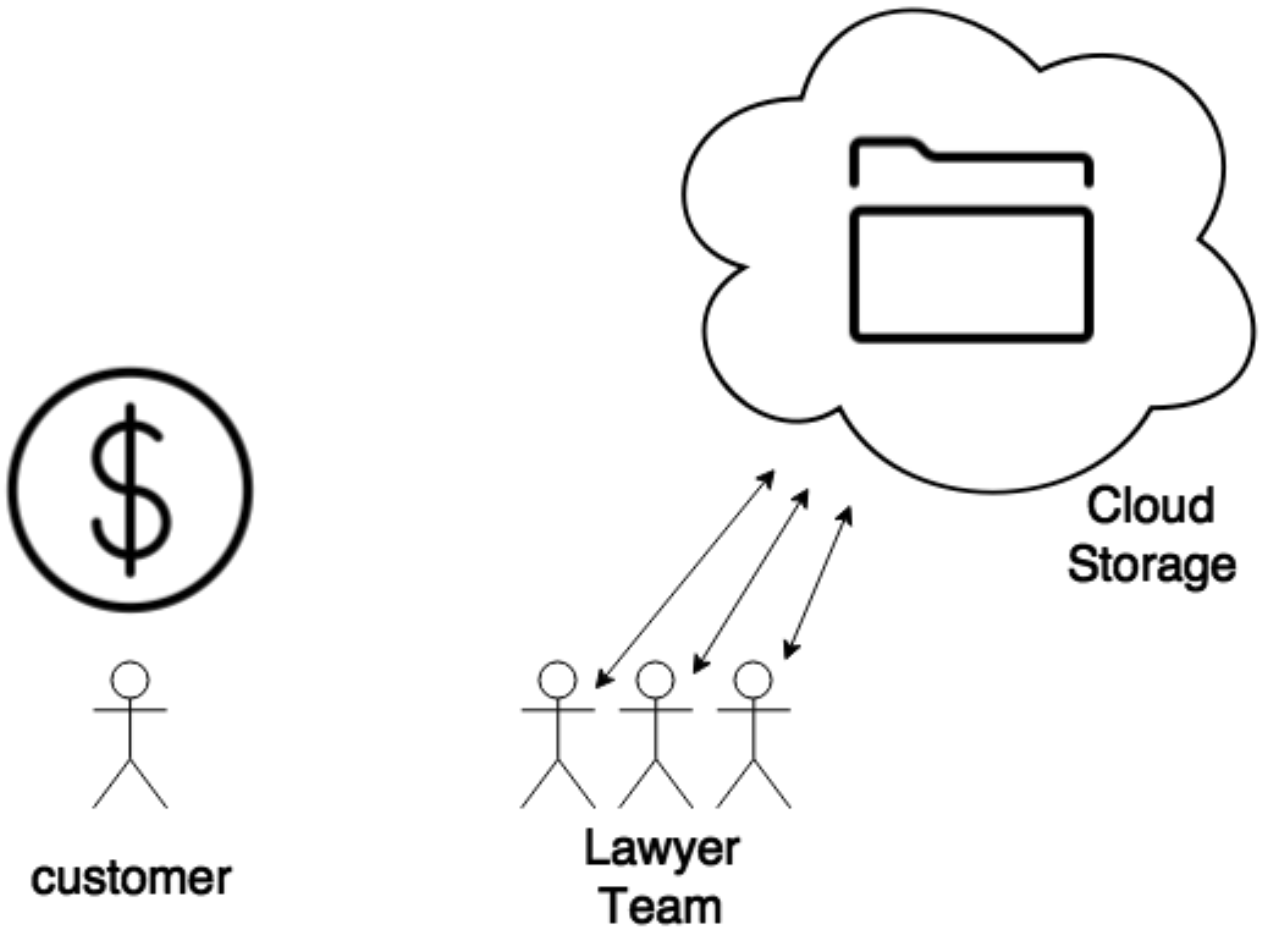
2015.12.31

Outline

Outline

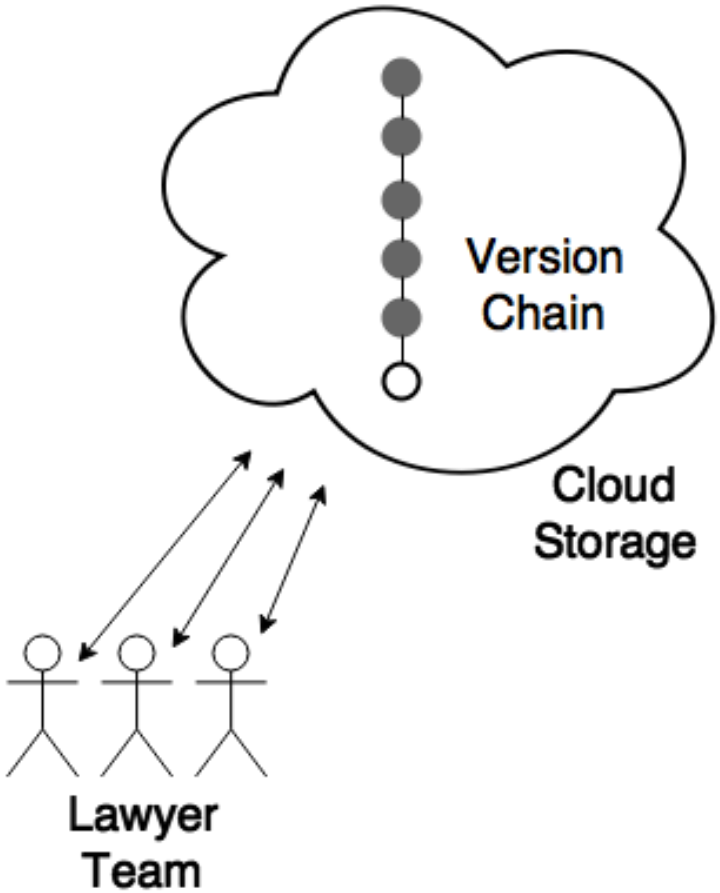
Scenario

Why Real-time Auditing?



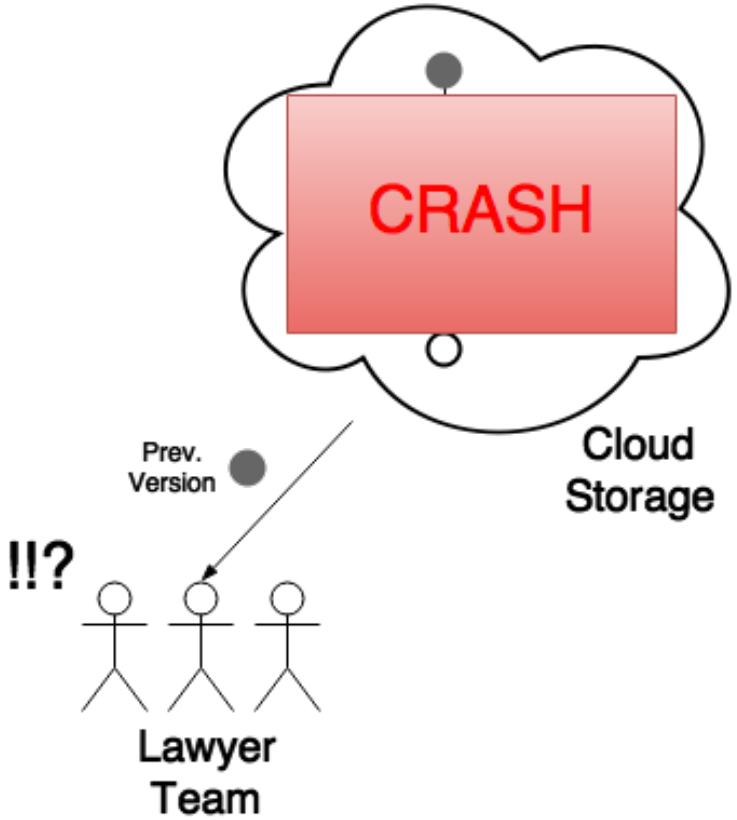
Scenario (CON'T)

Version Control



Scenario (CON'T)

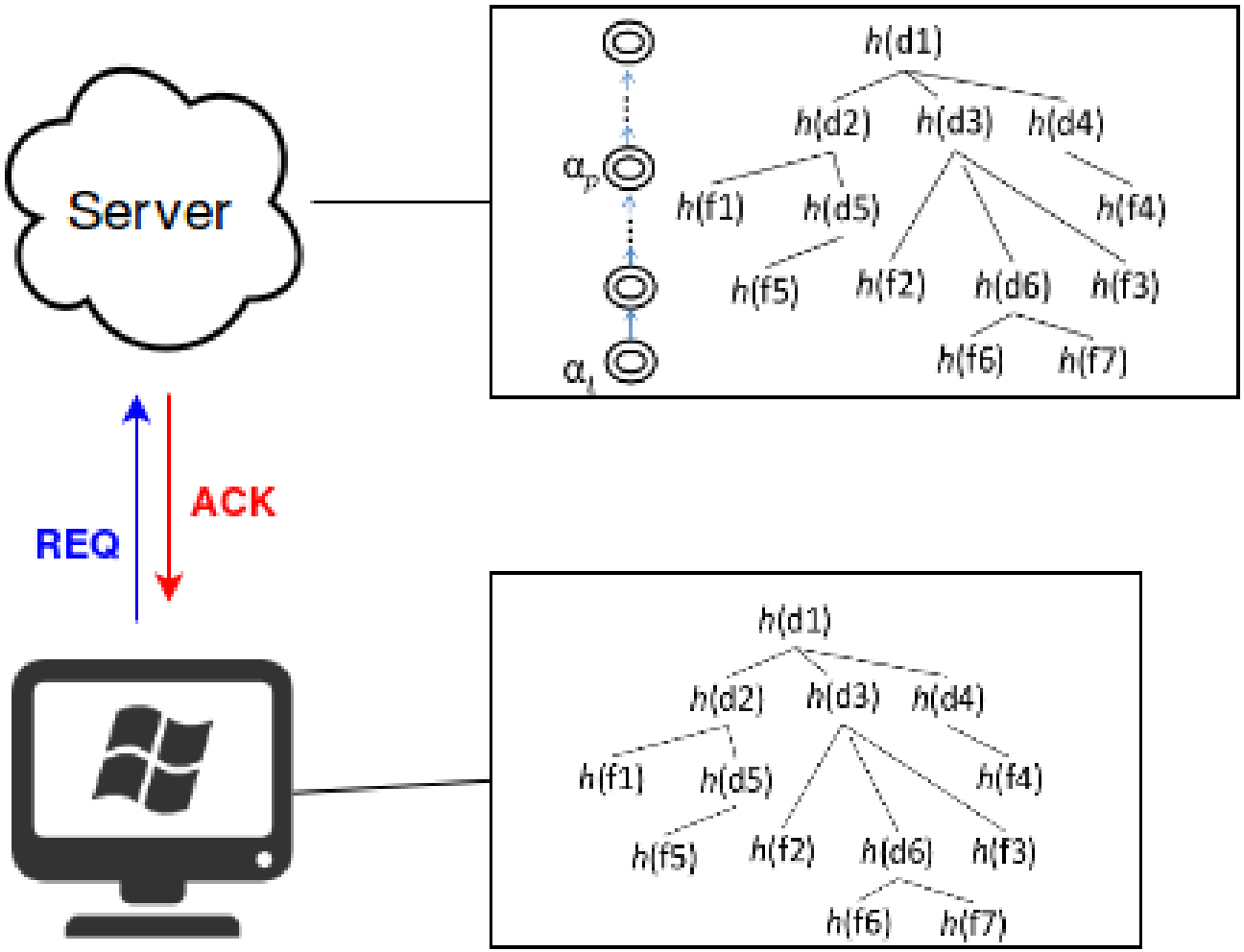
Problem



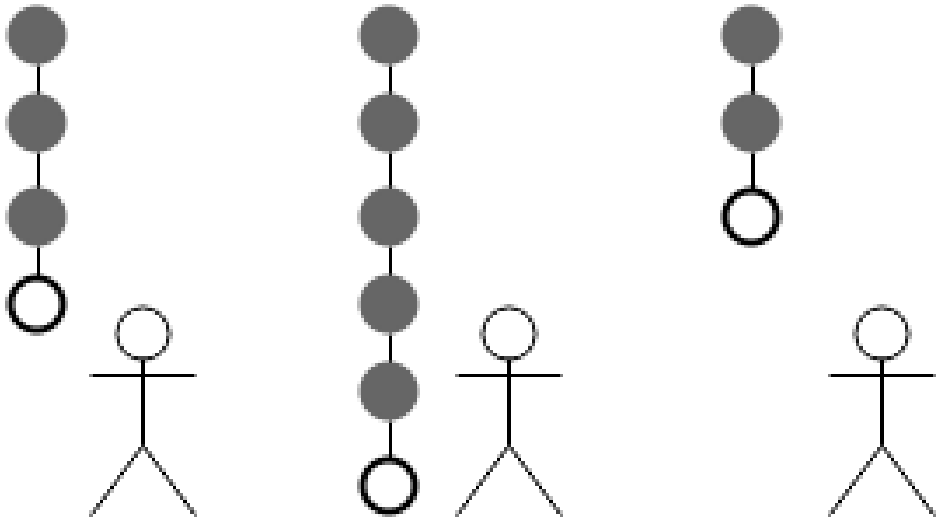
Cryptography Proof Needed

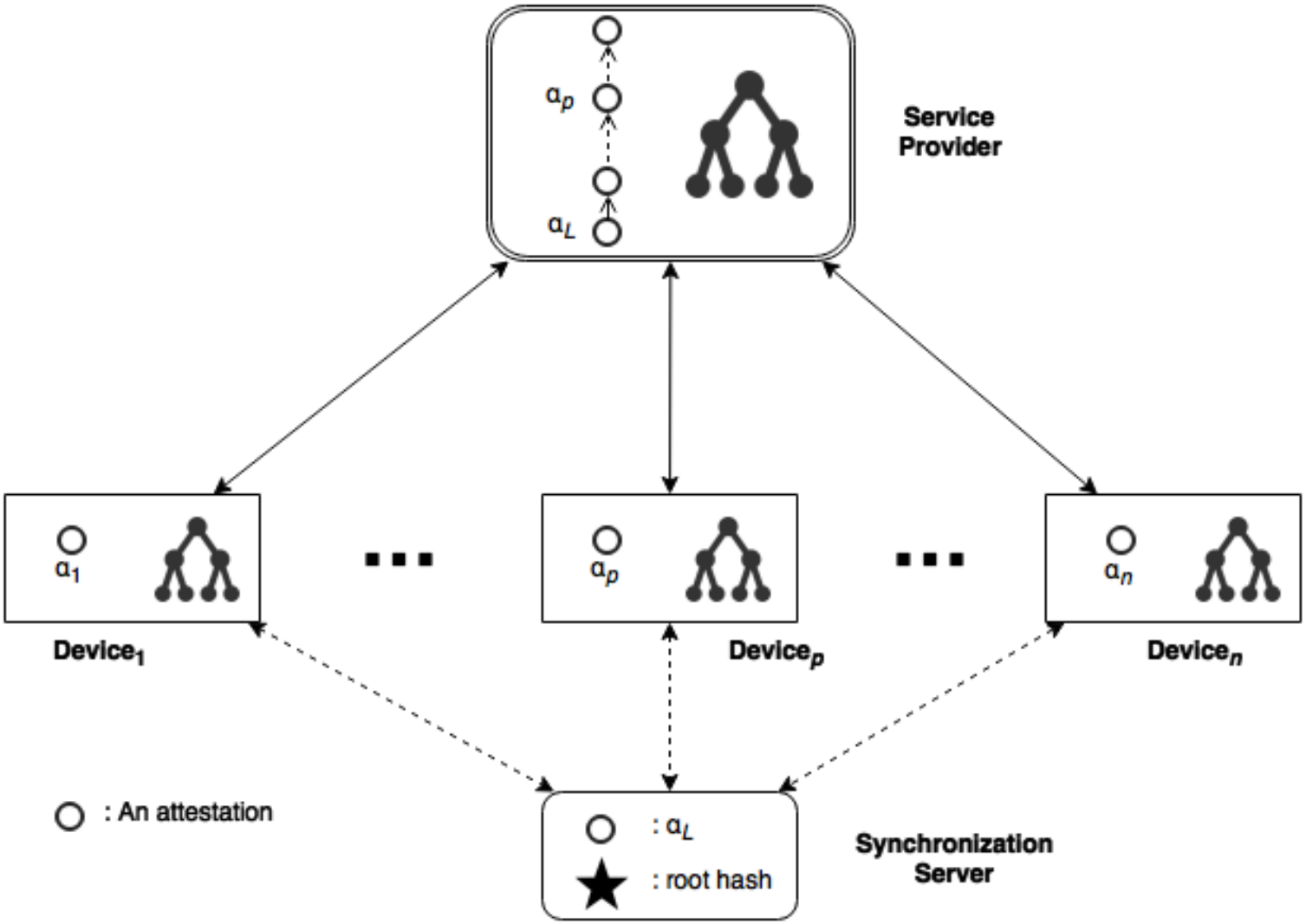
Outline

Intuitive Method

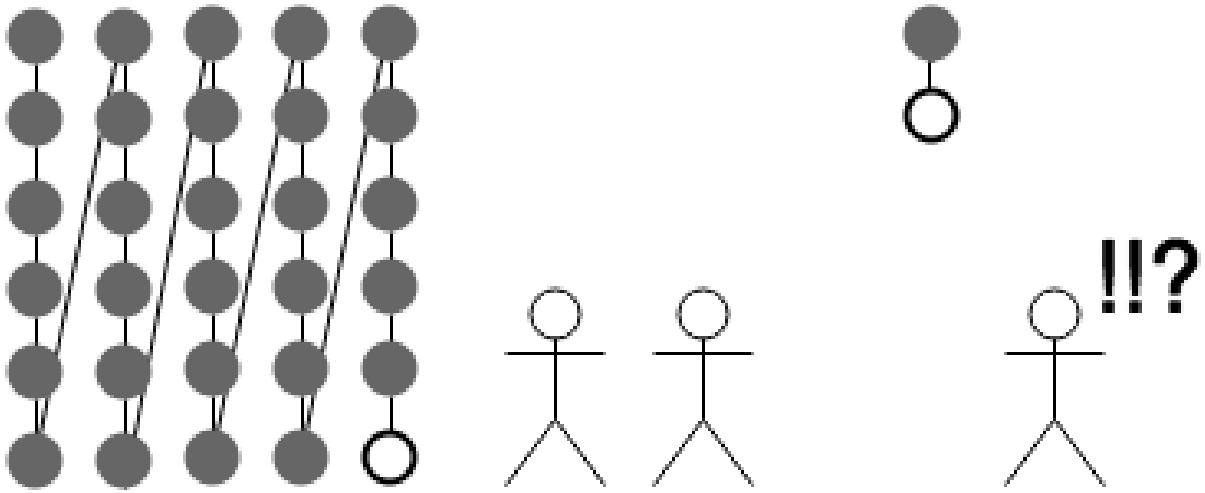


Problem




α_p
α_L
Service Provider
α_1
α_p
α_n
Device$_1$
Device$_p$
Device$_n$
: An attestation
: α_L
: root hash
Synchronization Server

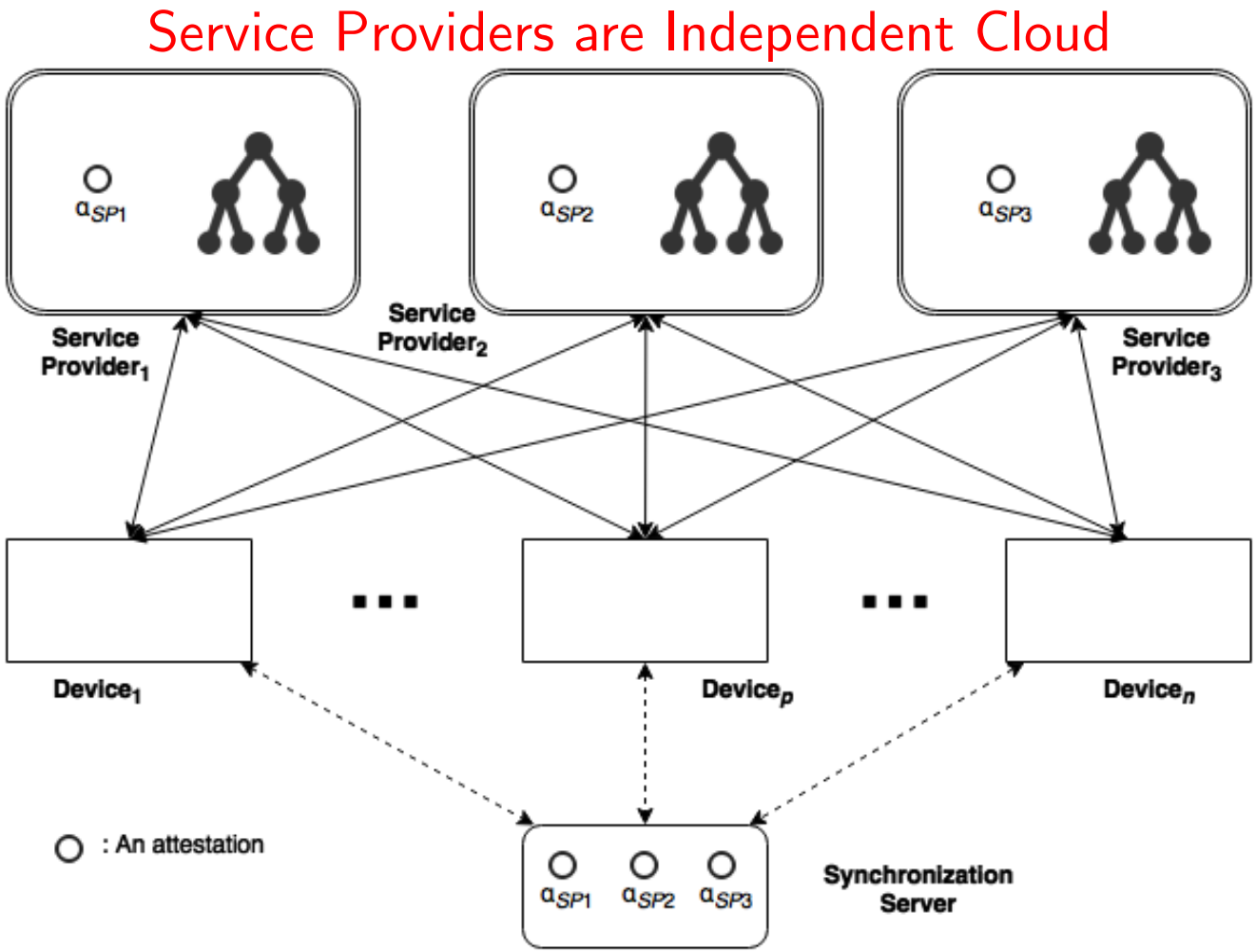
Worse-case



因爲要更新client端的Merkle Tree, 累積太多版本就需要很多時間來更新

My Method

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

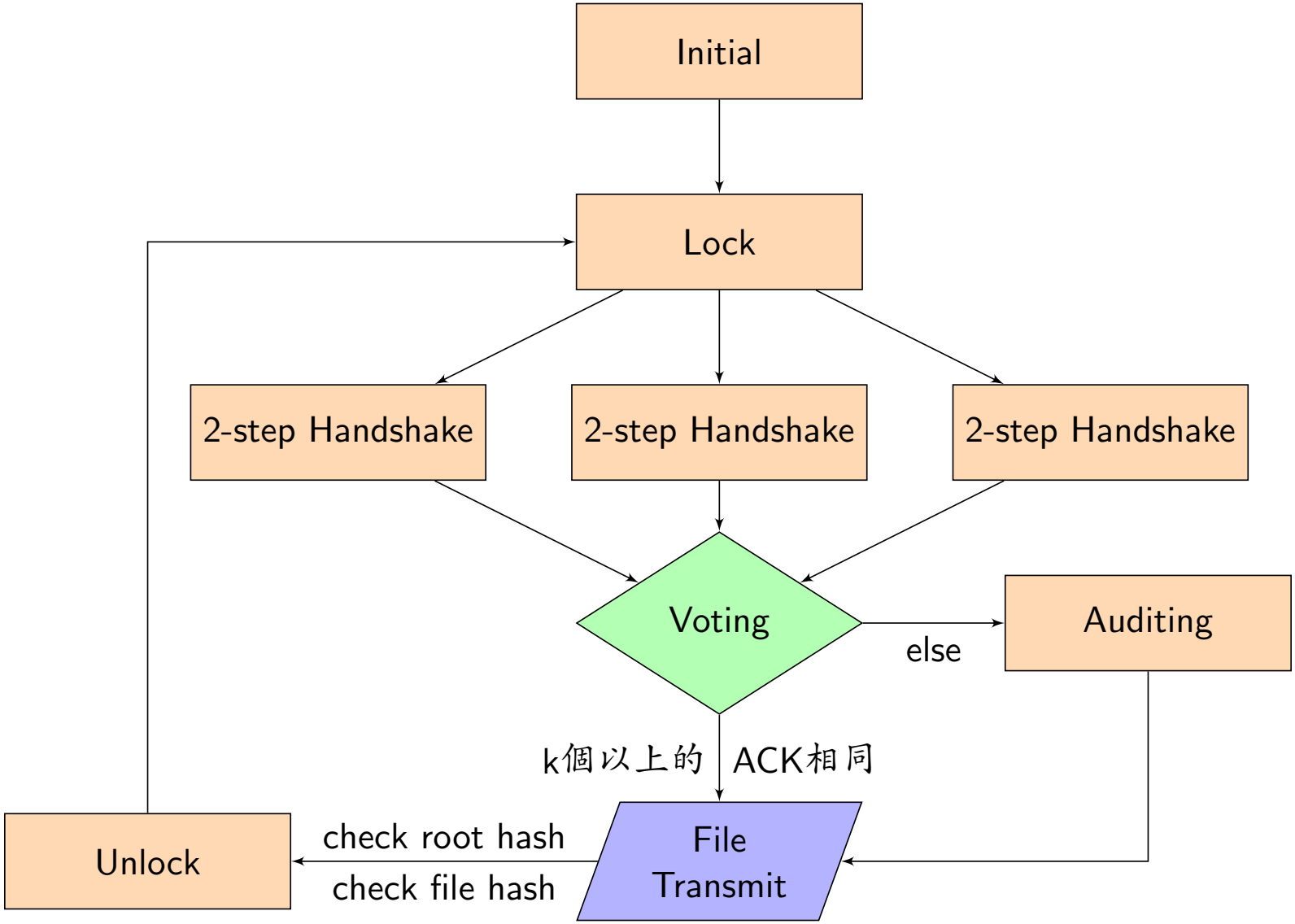


Comparison

- Pros
  1. Device 不用存 Merkle Tree, 省空間
  2. Device 也不用同步 Merkle Tree, 省時間
  3. 資料有多份備份
  4. 平均比之前的方法快速, 且沒有 Worse-case
- Cons
  1. 硬體成本較高
  2. 需要處理多份 Response

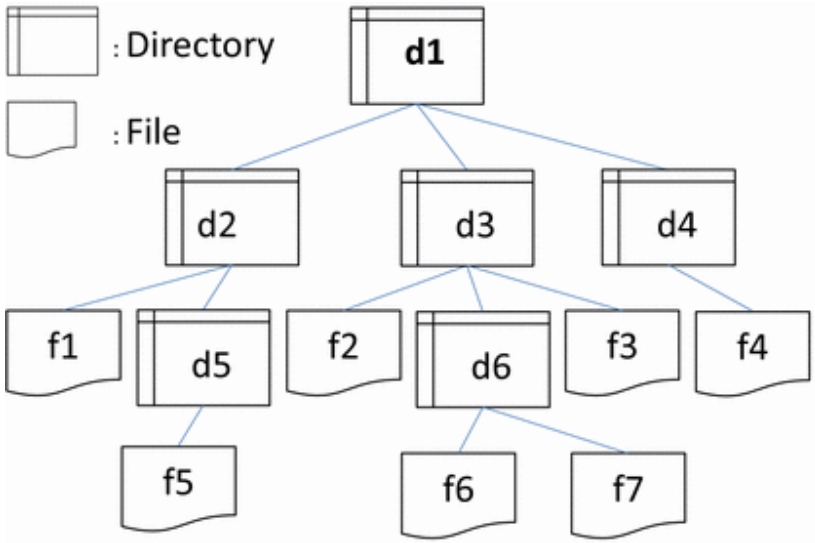
Outline

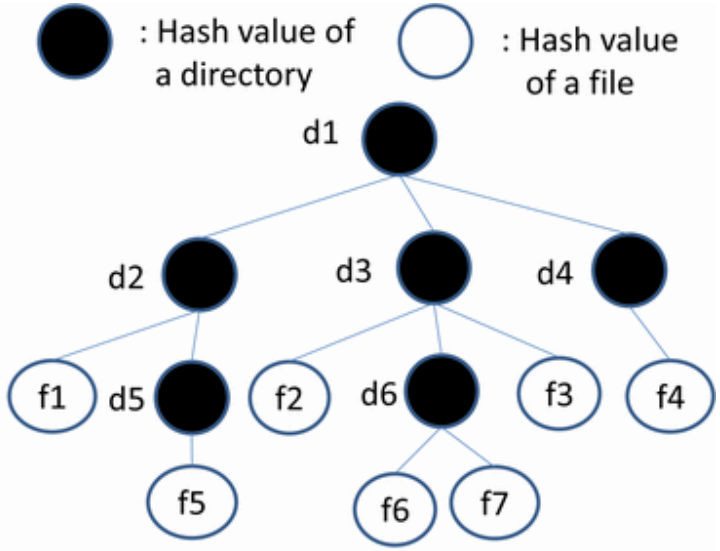
Flowchart


Initial
Lock
2-step Handshake
2-step Handshake
2-step Handshake
Voting
else
Auditing
k個以上的
ACK相同
Unlock
check root hash
check file hash
File
Transmit

Initial

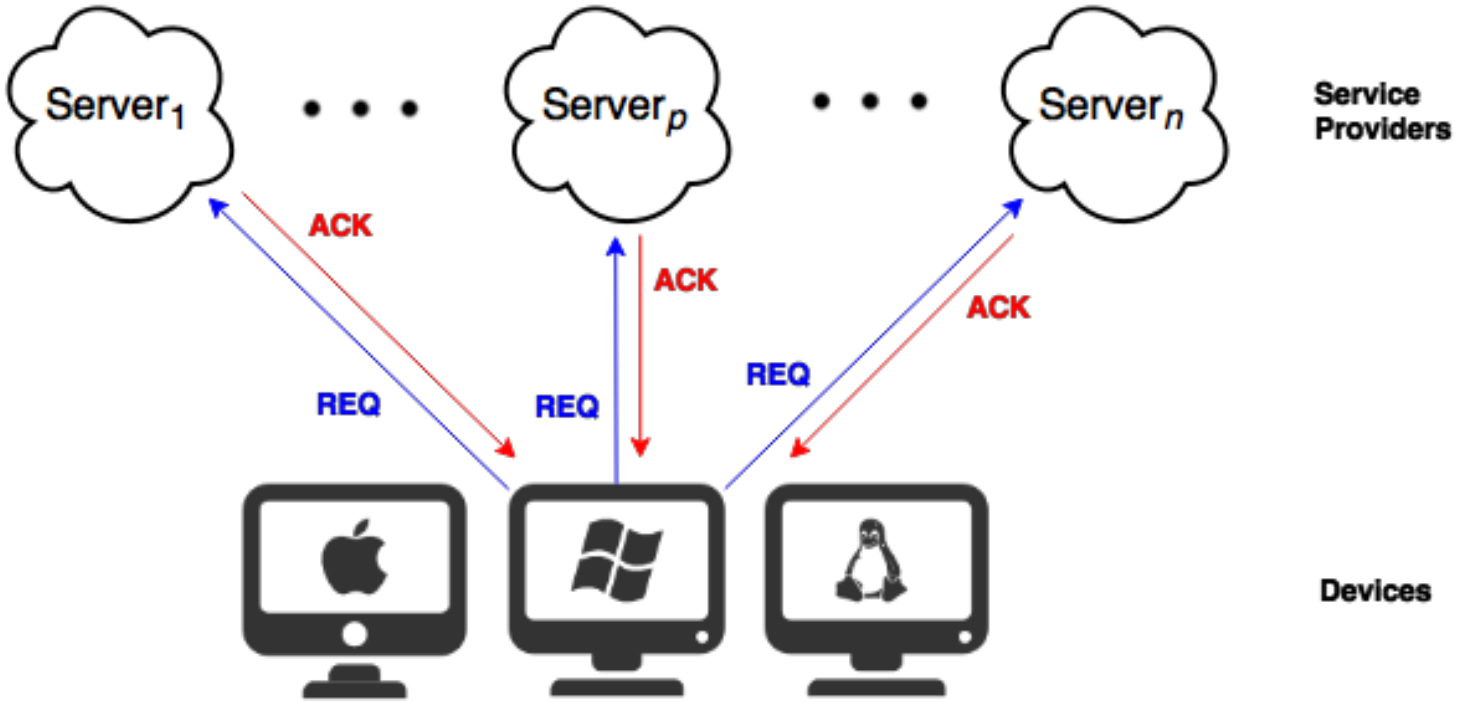
Create Merkle Tree





READ

I. 2-step Handshake & Voting

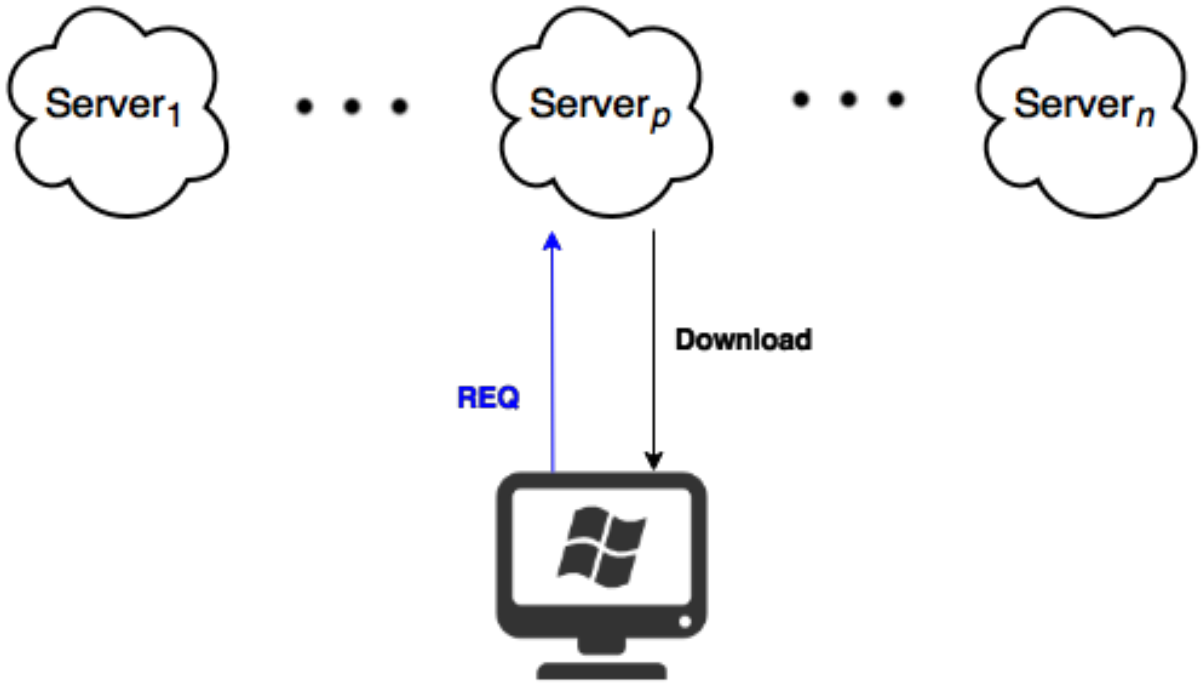


$$REQ = (op, [op]_{pri(D)})$$

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

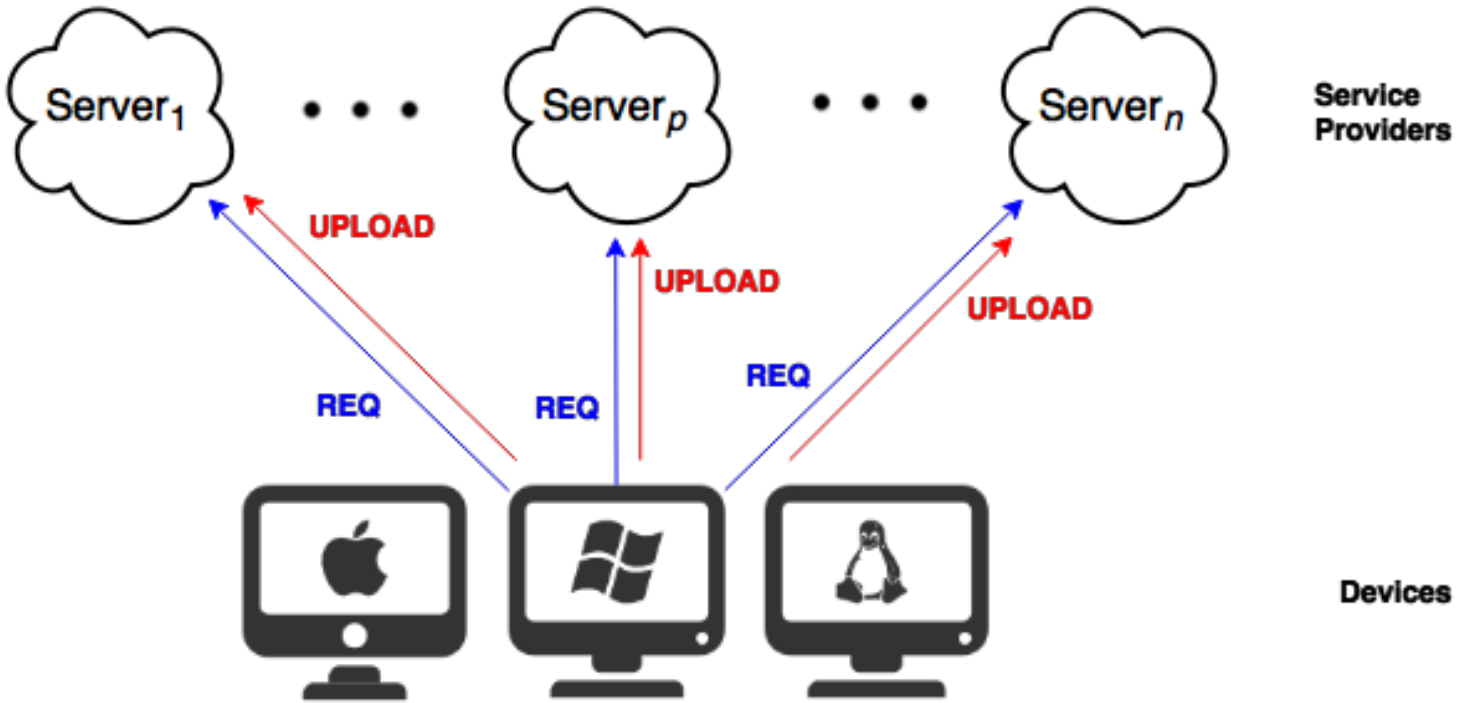
READ

II. Download



WRITE

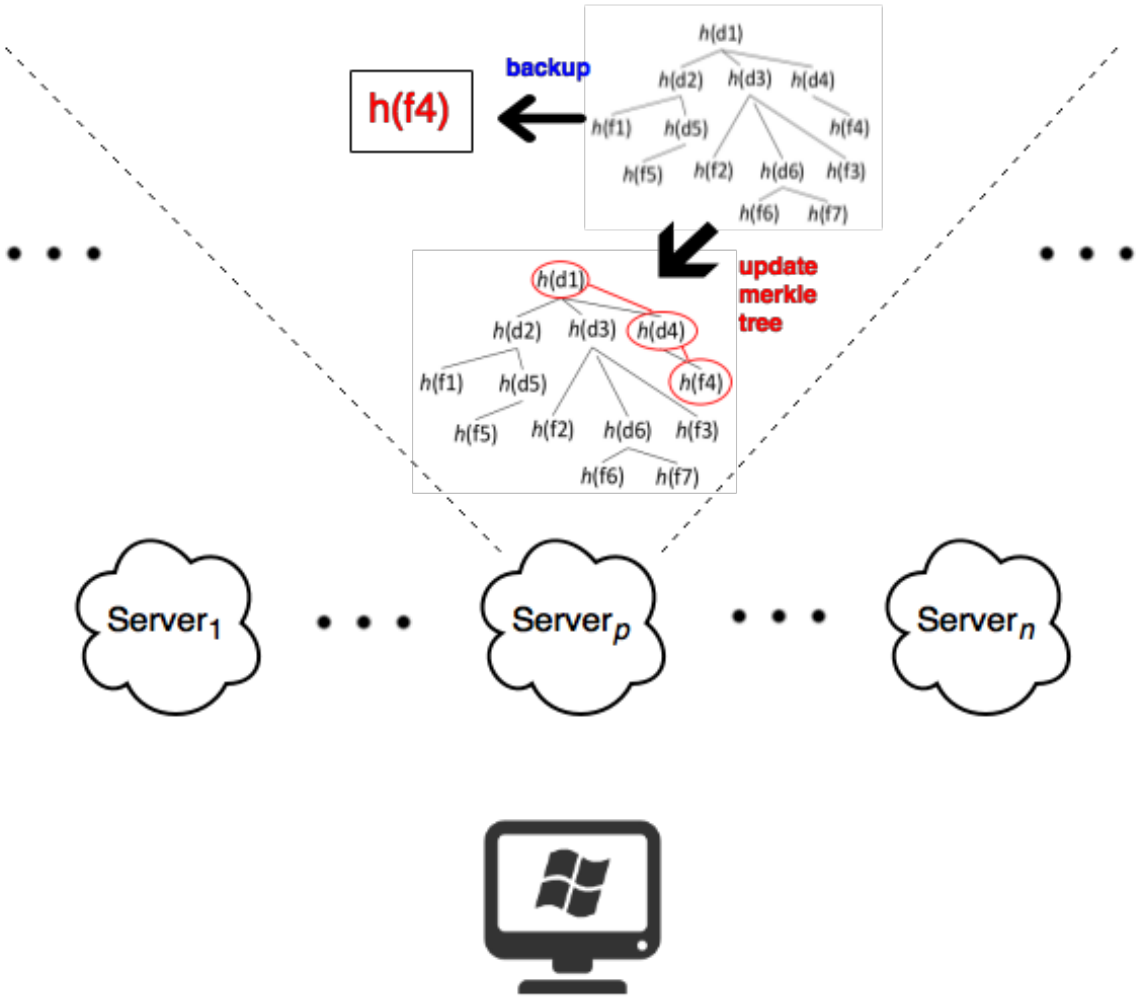
I. Upload



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

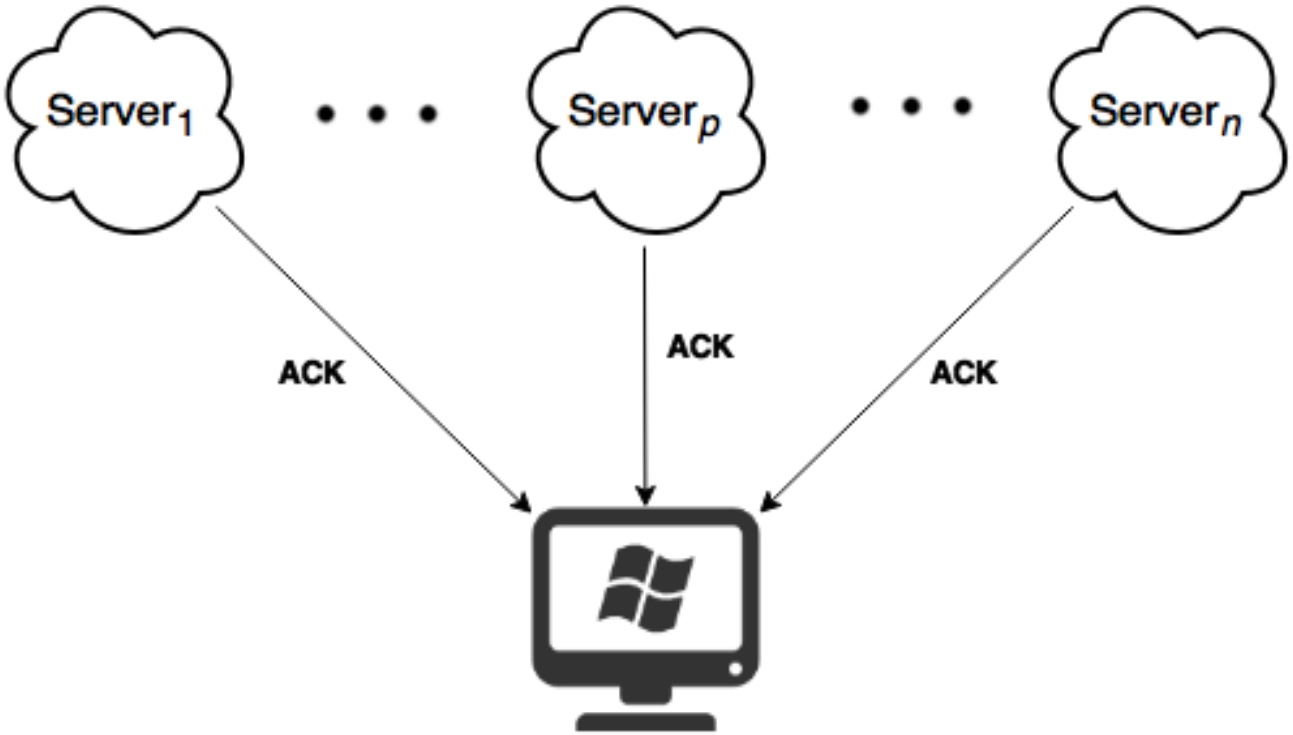
WRITE

II. Update Merkle Tree



WRITE

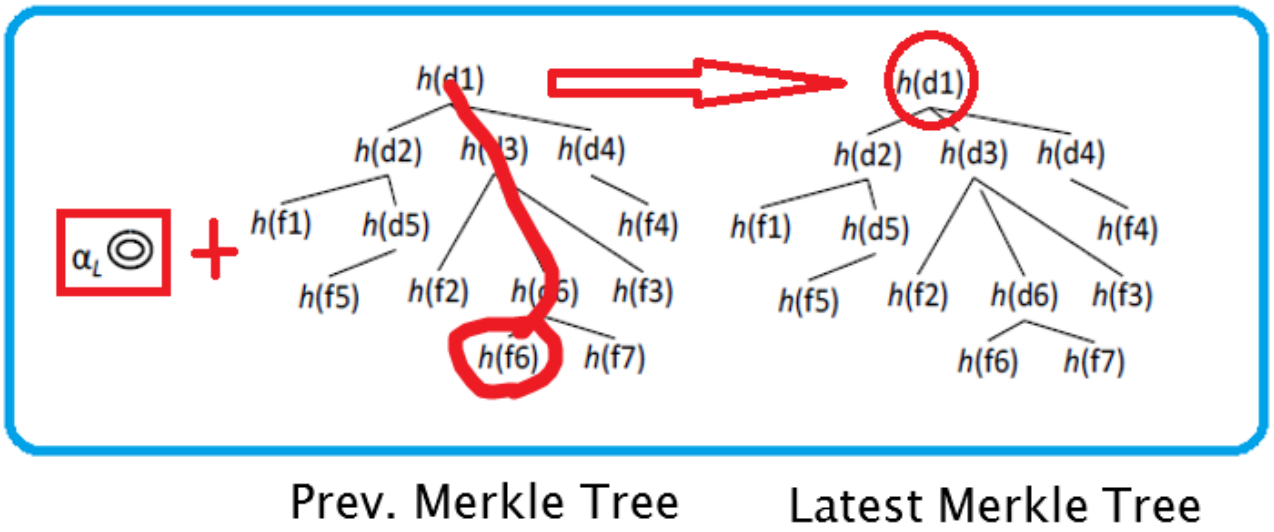
III. Voting



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

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

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.
   - Acknowledgement Chain Implements.
3. Question: Read Operation slower than Write Operation
4. Design Different Experiments.

Outline

Experimental Results

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

Account A		666MB	42files	6dirs.	
Test Data	1KB	10KB	100KB	1MB	10MB
Non POV					
READ	0.72	0.519	0.471	1.766	13.417
WRITE	1.086	0.651	1.891	3.172	16.426
Wei Chih					
READ	2.575	13.94	3.047	5.353	40.18
WRITE	3.354	2.79	3.608	9.376	65.731
Wei Shain					
READ	1.982	1.756	3.325	6.477	40.606
WRITE	1.708	2.046	3.67	4.834	16.574

Server and Client on the Same Machine

Thank You!