Instant Auditing of Cloud Storage Access by Voting of Different Cloud Storages

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

NTNU CSIE CCLAB

2016.05.24

Outline

1. Scenario
2. Real-time Auditing Schemes
   - Instant Auditing of Cloud Storage Access by Cache Partial Merkle tree
   - My Method
3. Protocol Detail
   - Flowchart
   - Download & Upload
   - Audit
4. Experimental Results

Outline

1. Scenario

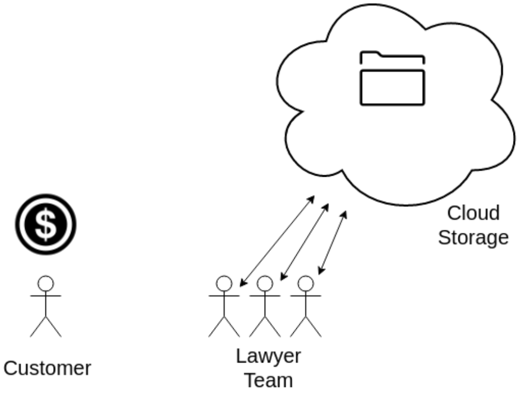
2. Real-time Auditing Schemes
   - Instant Auditing of Cloud Storage Access by Cache Partial Merkle tree
   - My Method

3. Protocol Detail
   - Flowchart
   - Download & Upload
   - Audit

4. Experimental Results

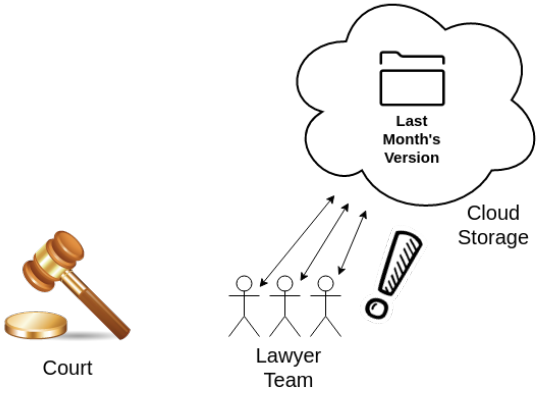
Scenario

Law Office



Scenario (CON'T)

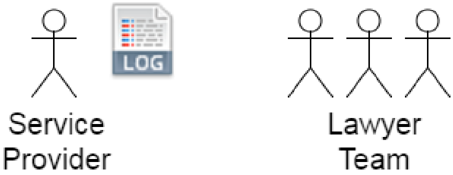
What if...



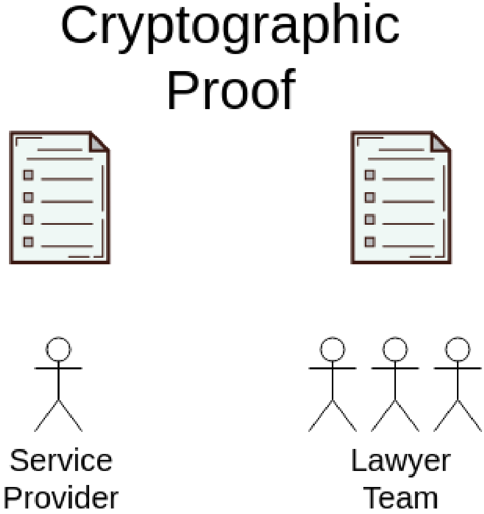
Scenario (CON'T)

No Error !

No Evidence ...



Scenario (CON'T)



Outline

1. Scenario

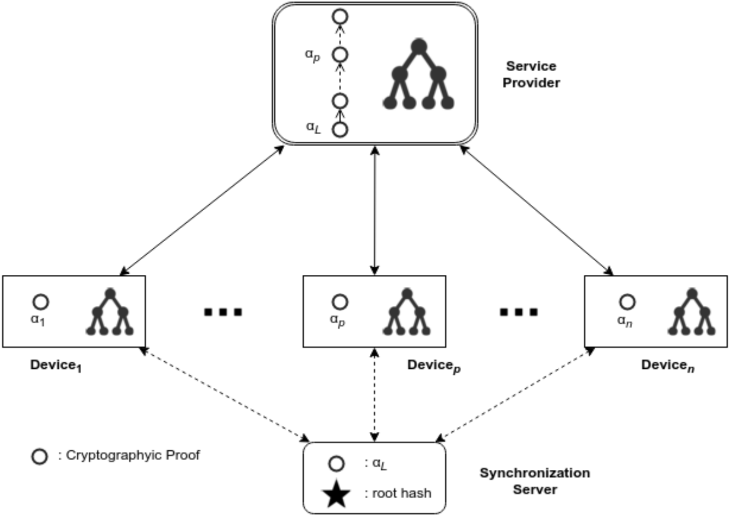
2. Real-time Auditing Schemes
   - Instant Auditing of Cloud Storage Access by Cache Partial Merkle tree
   - My Method

3. Protocol Detail
   - Flowchart
   - Download & Upload
   - Audit

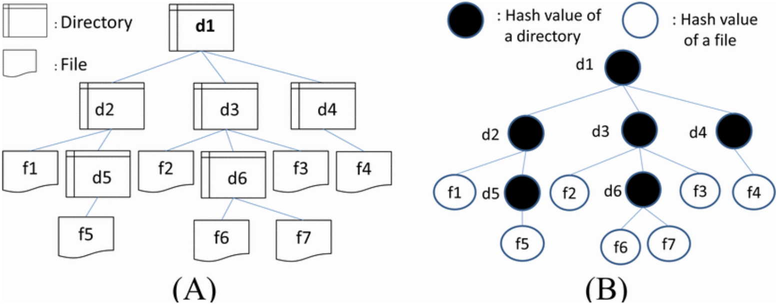
4. Experimental Results

Instant Auditing of Cloud Storage Access by Cache Partial Merkle tree

2014 IEEE 6th International Conference on Cloud Computing Technology and Science



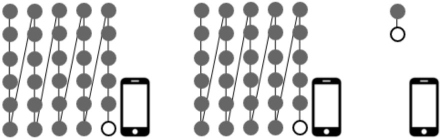
Merkle Tree


: Directory
: File
d1
d2
d3
d4
f1
d5
f2
d6
f3
f4
f5
f6
f7
(A)
: Hash value of a directory
: Hash value of a file
d1
d2
d3
d4
f1
d5
f2
d6
f3
f4
f5
f6
f7
(B)

Worst-case

若有個 device 很久沒有使用，在讀寫檔案前需要更新大量未做的動作

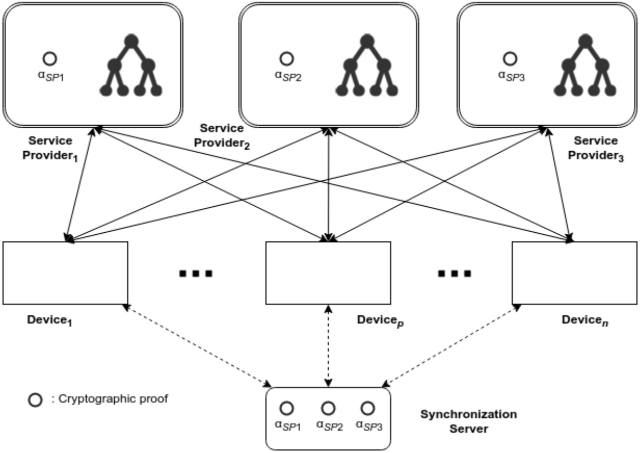
使用者將會明顯感受到漫長的等待時間



My Method

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

Service Providers are Independent Cloud



Comparison

- Pros
  1. Device 不用儲存、也不用修改 Merkle tree, 既省空間又省時間
  2. 資料有多份備份
  3. 解決之前的 Worst-case
- Cons
  1. 需要傳送多份 Request, 處理多份 Response

Outline

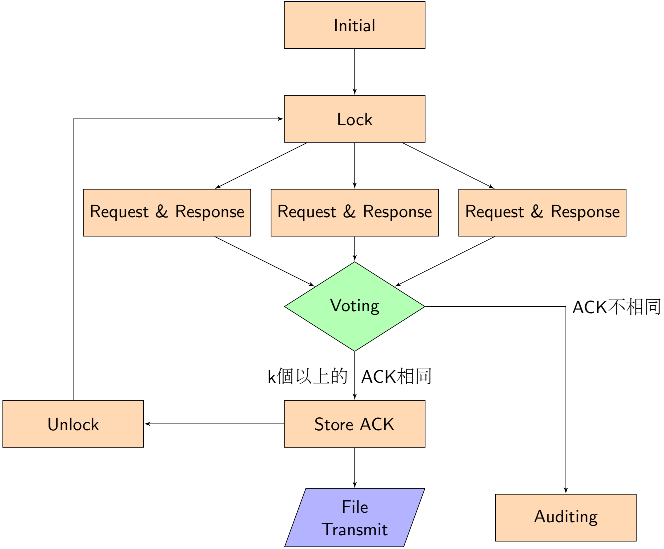
1. Scenario

2. Real-time Auditing Schemes
   - Instant Auditing of Cloud Storage Access by Cache Partial Merkle tree
   - My Method

3. Protocol Detail
   - Flowchart
   - Download & Upload
   - Audit

4. Experimental Results

Flowchart



Initial

Lock

Request & Response

Request & Response

Request & Response

Voting

ACK不相同

k個以上的 ACK相同

Unlock

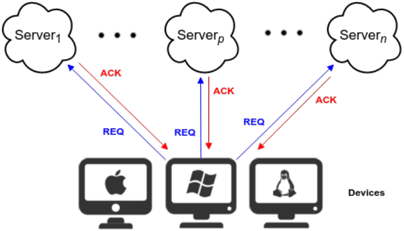
Store ACK

File Transmit

Auditing

Download & Upload

Request & Response



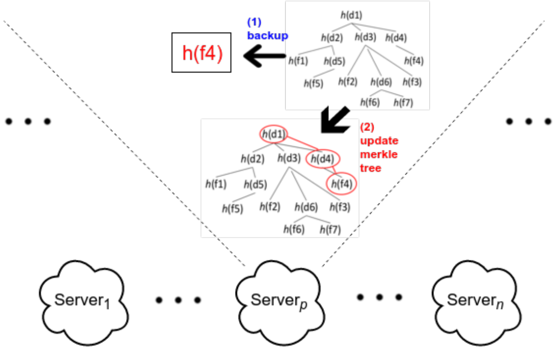
$$REQ = (OP,\ [OP]_{pri(D)})$$
$$OP = (TYPE,\ PATH,\ HASH)$$

$$ACK = (RESULT,\ REQ,\ [RESULT,\ REQ]_{pri(S)})$$
$$RESULT = (roothash,\ filehash)$$

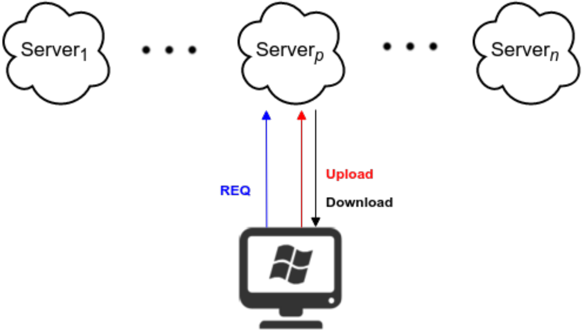
collect ACKs and voting

if Operation is UPLOAD

Server Update Merkle tree



File Transmit



Audit

$\because$ ACK 中有 roothash
$\therefore$ 新的 request 之前，所有的檔案都經過檢查，沒有問題

device request OP_i，收到回傳的 ACK_i
發現 $Server_p$ 的 ACK 有錯誤，因此向 $Server_p$ 稽核

device 向 $Server_p$ 索取 MT_{i-1}
(MT_{i-1} 為執行 OP_i 之前的 Merkle tree)

①② 兩點有一個出錯就能確定 $Server_p$ 出錯

① device 檢查 MT_{i-1} 的 roothash 應和 ACK_{i-1} 中的 roothash 一樣

② device 以 OP_i 中的 hash value 來更新 MT_{i-1}，
更新後的 roothash 應和 $Server_p$ 現在的 roothash 相同

Outline

1. Scenario
2. Real-time Auditing Schemes
   - Instant Auditing of Cloud Storage Access by Cache Partial Merkle tree
   - My Method
3. Protocol Detail
   - Flowchart
   - Download & Upload
   - Audit
4. Experimental Results

Experimental Results

	Size	File	Directory	Merkle tree Size
A	777 MB	48	6	5.4 KB
B	145 MB	54198	188	5.08 MB
C	5.95 GB	45089	1459	4.37 MB

Table: GENERATE MERKLE TREE'S TIME (IN SEC.)

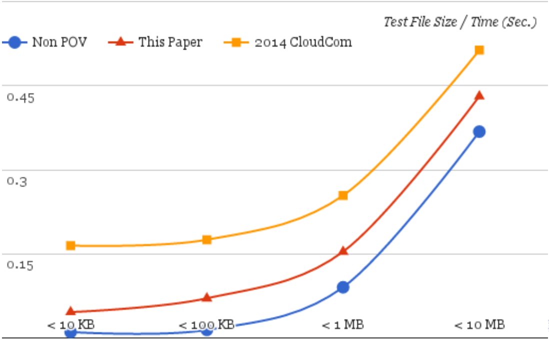
		A	B	C
PC	Generate	14.876	61.176	198.405
	Serialize	0.040	0.756	0.670
	Deserialize	0.009	0.299	0.295
VM	Generate	6.821	144.267	620.151
	Serialize	0.011	0.343	0.299
	Deserialize	0.015	1.016	0.860

Experimental Results

The client device and SP are in the same network segment

Table: THE EXECUTION TIME OF UPLOAD OPERATIONS (IN SEC.) (Account C)

Test File	Non POV	This Paper	2014 CloudCom
<10 KB	0.010608	0.046139	0.164744
<100 KB	0.014393	0.070739	0.175226
<1 MB	0.090440	0.153822	0.253963
<10 MB	0.367989	0.430937	0.513308



Experimental Results

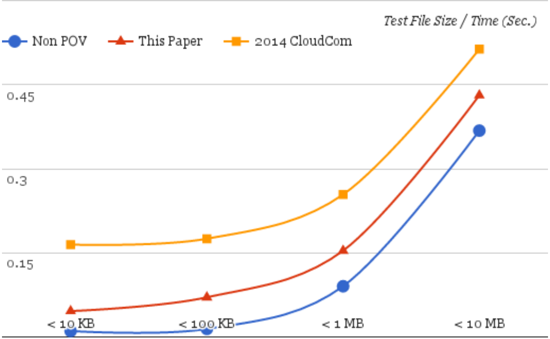
The client device and SP are in the same network segment (UPLOAD)

Table:

Test File	Rate
<10 KB	-76.95%
<100 KB	-64.97%
<1 MB	-61.24%
<10 MB	-56.68%

$$Rate = \frac{(V-N) - (C-N)}{(C-N)}$$

$$V = Voting, \ this \ paper$$
$$C = 2014 \ Cloud \ Com$$
$$N = Non \ POV$$

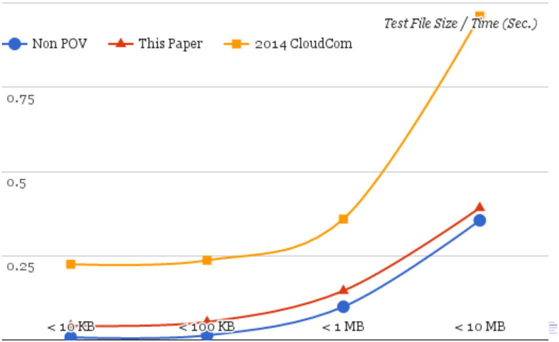


Experimental Results

The client device and SP are in the same network segment

Table: THE EXECUTION TIME OF DOWNLOAD OPERATIONS (IN SEC.) (Account C)

Test File	Non POV	This Paper	2014 CloudCom
<10 KB	0.007845	0.042295	0.224947
<100 KB	0.013691	0.053583	0.236347
<1 MB	0.098570	0.146021	0.359045
<10 MB	0.354916	0.392072	0.961740



Experimental Results

The client device and SP are in the same network segment (DOWNLOAD)

Table:

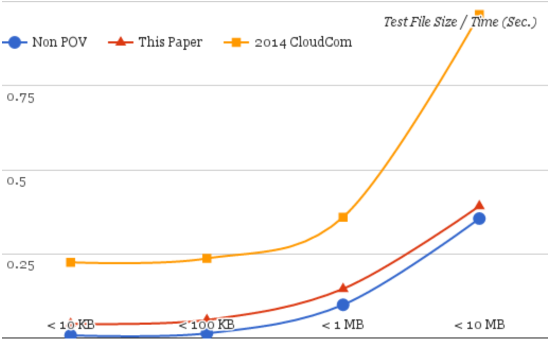
Test File	Rate
<10 KB	-84.13%
<100 KB	-82.08%
<1 MB	-81.78%
<10 MB	-93.88%

$$Rate = \frac{(V-N) - (C-N)}{(C-N)}$$

$$V = Voting, \ this \ paper$$

$$C = 2014 \ Cloud \ Com$$

$$N = Non \ POV$$

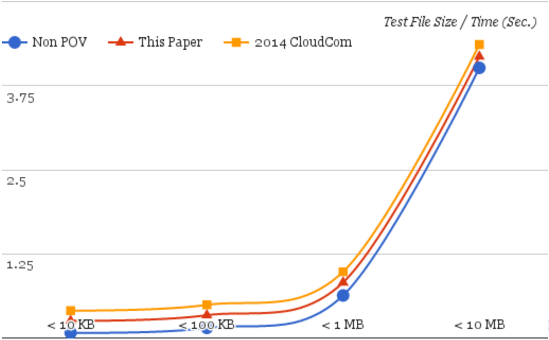


Experimental Results

The client device and SP are not in the same network segment

Table: THE EXECUTION TIME OF UPLOAD OPERATIONS (IN SEC.) (Account C)

Test File	Non POV	This Paper	2014 CloudCom
<10 KB	0.077653	0.254801	0.407407
<100 KB	0.149493	0.338238	0.492000
<1 MB	0.631626	0.825261	0.983832
<10 MB	4.014217	4.182142	4.359997



Experimental Results

The client device and SP are not in the same network segment (UPLOAD)

Table:

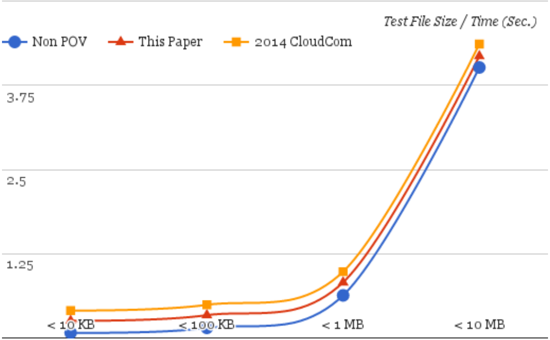
Test File	Rate
<10 KB	-46.28%
<100 KB	-44.89%
<1 MB	-45.02%
<10 MB	-51.44%

$$Rate = \frac{(V-N) - (C-N)}{(C-N)}$$

$$V = Voting,\ this\ paper$$

$$C = 2014\ Cloud\ Com$$

$$N = Non\ POV$$

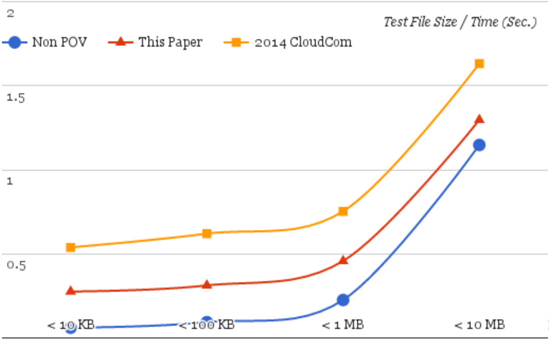


Experimental Results

The client device and SP are not in the same network segment

Table: THE EXECUTION TIME OF DOWNLOAD OPERATIONS (IN SEC.) (Account C)

Test File	Non POV	This Paper	2014 CloudCom
<10 KB	0.061063	0.275808	0.538531
<100 KB	0.093941	0.312340	0.620296
<1 MB	0.225640	0.457329	0.752591
<10 MB	1.147272	1.296215	1.631534



Experimental Results

The client device and SP are not in the same network segment (DOWNLOAD)

Table:

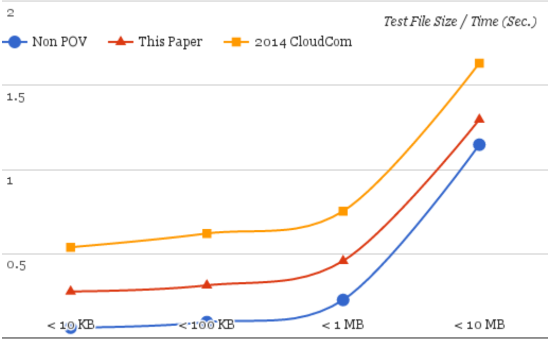
Test File	Rate
<10 KB	-55.02%
<100 KB	-58.51%
<1 MB	-56.03%
<10 MB	-69.24%

$$Rate = \frac{(V-N) - (C-N)}{(C-N)}$$

$$V = Voting,\ this\ paper$$

$$C = 2014\ Cloud\ Com$$

$$N = Non\ POV$$

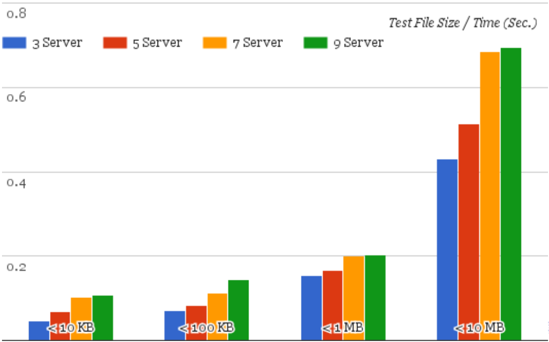


Experimental Results

Running time of different numbers' servers

Table: THE EXECUTION TIME OF UPLOAD OPERATIONS (IN SEC.) (Account C)

Test File	3 Server	5 Server	7 Server	9 Server
<10 KB	0.046139	0.067923	0.101676	0.108696
<100 KB	0.070739	0.083563	0.112895	0.145049
<1 MB	0.153822	0.166289	0.200053	0.203870
<10 MB	0.430937	0.513879	0.684666	0.694259

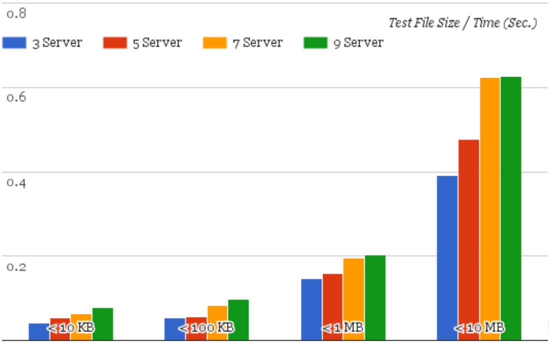


Experimental Results

Running time of different numbers' servers

Table: THE EXECUTION TIME OF DOWNLOAD OPERATIONS (IN SEC.) (Account C)

Test File	3 Server	5 Server	7 Server	9 Server
<10 KB	0.042295	0.054263	0.064370	0.078872
<100 KB	0.053583	0.055442	0.083961	0.097507
<1 MB	0.146021	0.159869	0.195817	0.202213
<10 MB	0.392072	0.476251	0.622665	0.625499



Thank
You!