利用備份與投票技術實作雲端儲存之即時行為違反證明技術

Implementing Real-time POV for Cloud Storage by Replication and Voting

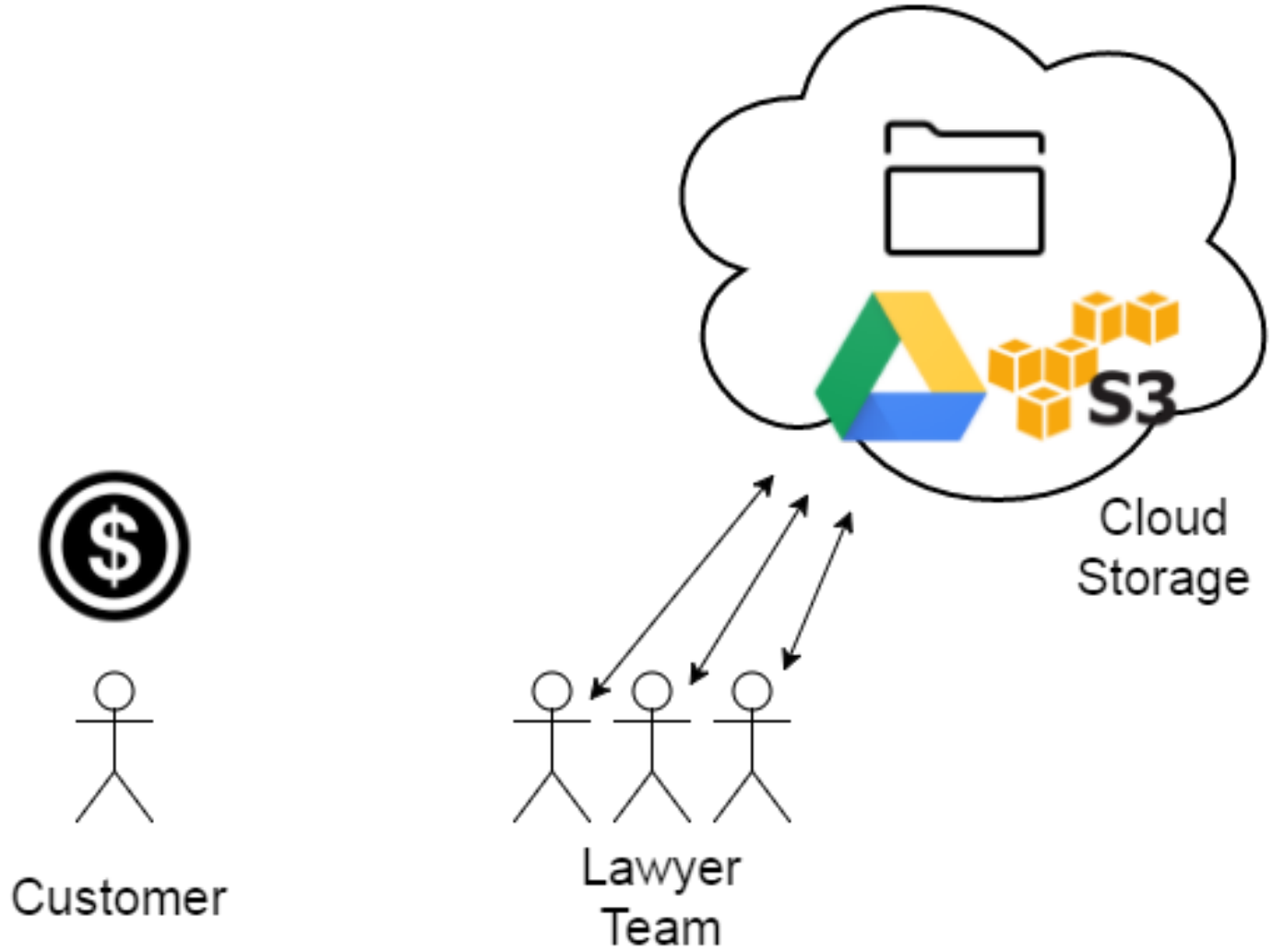
Adviser : Gwan-Hwan Hwang
Student : Wei-Chih Chien

NTNU CSIE CCLAB

2016.07.13

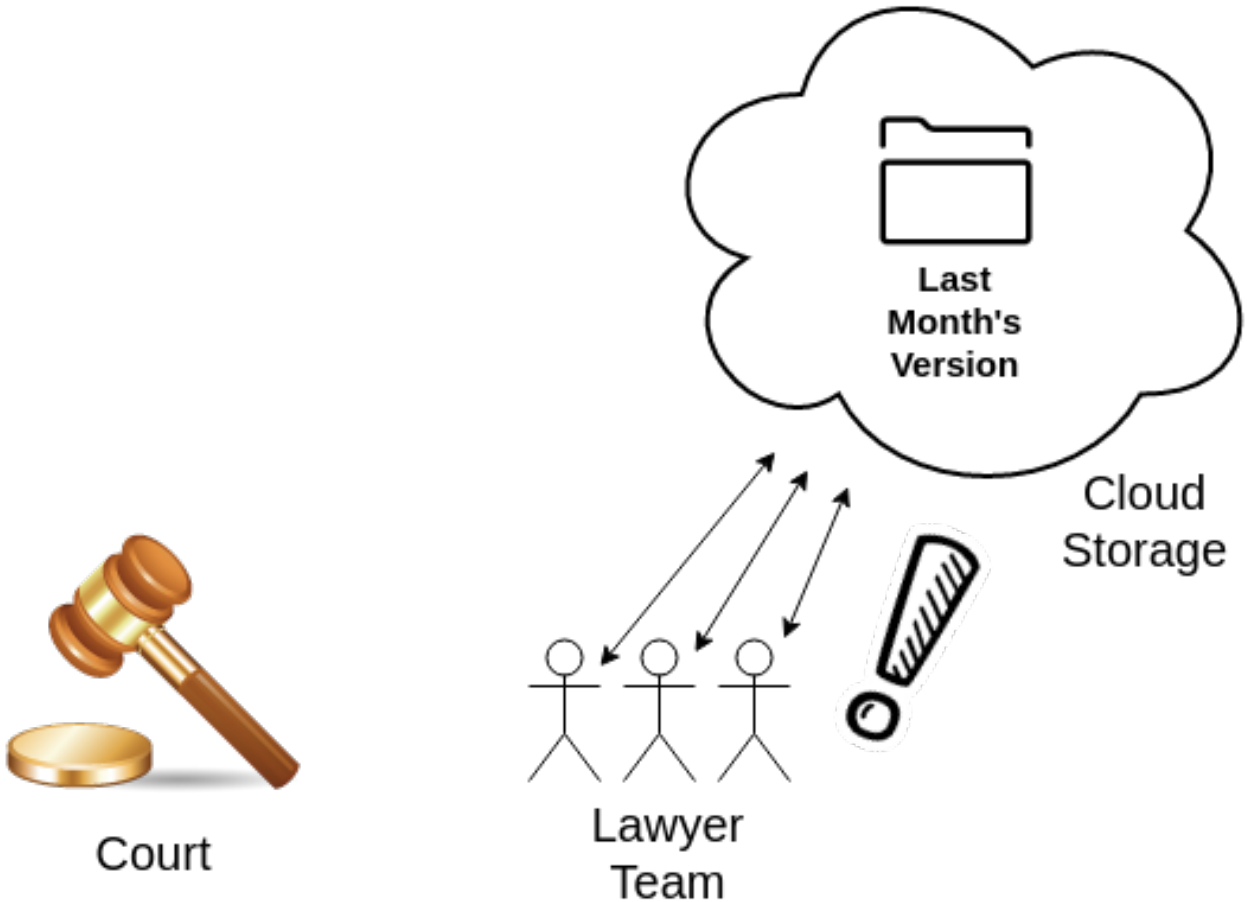
Outline

Scenario
Law Office



Scenario (CON'T)

What if...

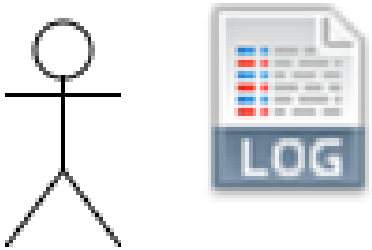


Service Provider's Rollback Attack

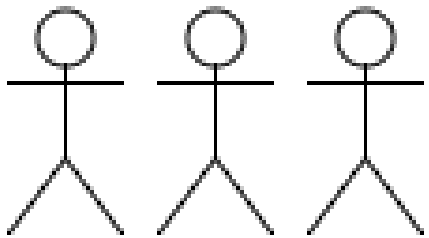
Scenario (CON'T)

No Error !

No Evidence ...

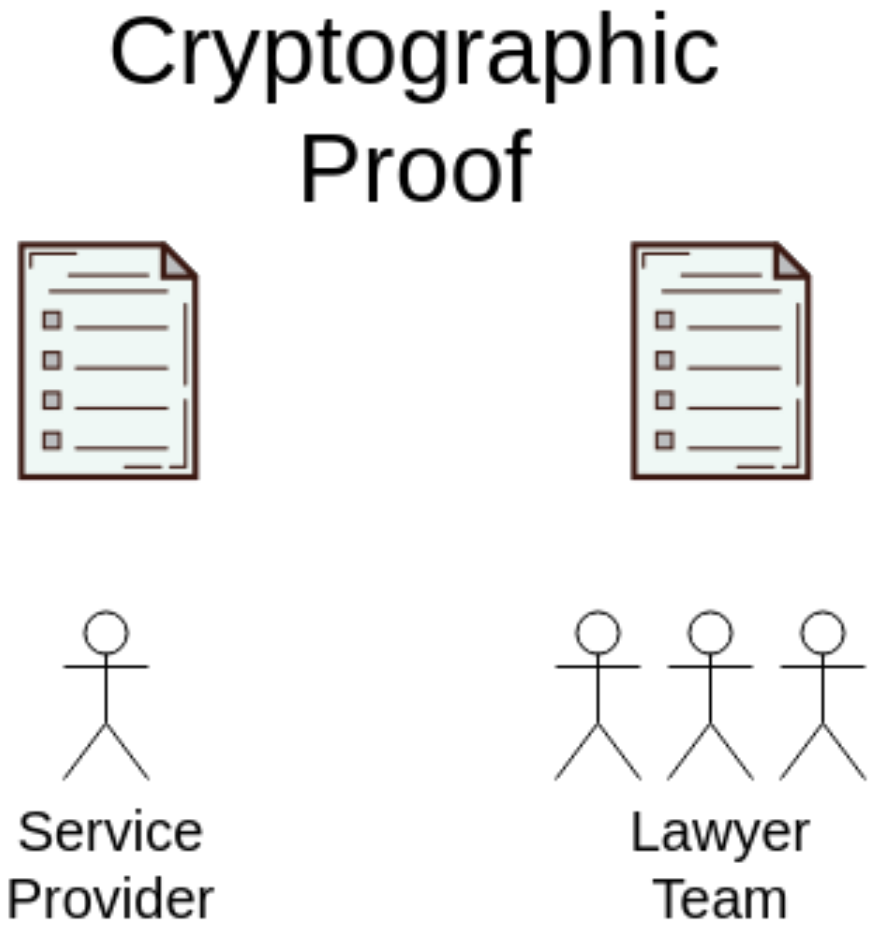


Service Provider



Lawyer Team

Scenario (CON'T)



Obtaining Mutual Non-repudiation

Previous Work

Hwang, Gwan-Hwan, Wei-Sian Huang, and Jenn-Zjone Peng. "Real-time proof of violation for cloud storage." Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on. IEEE, 2014.

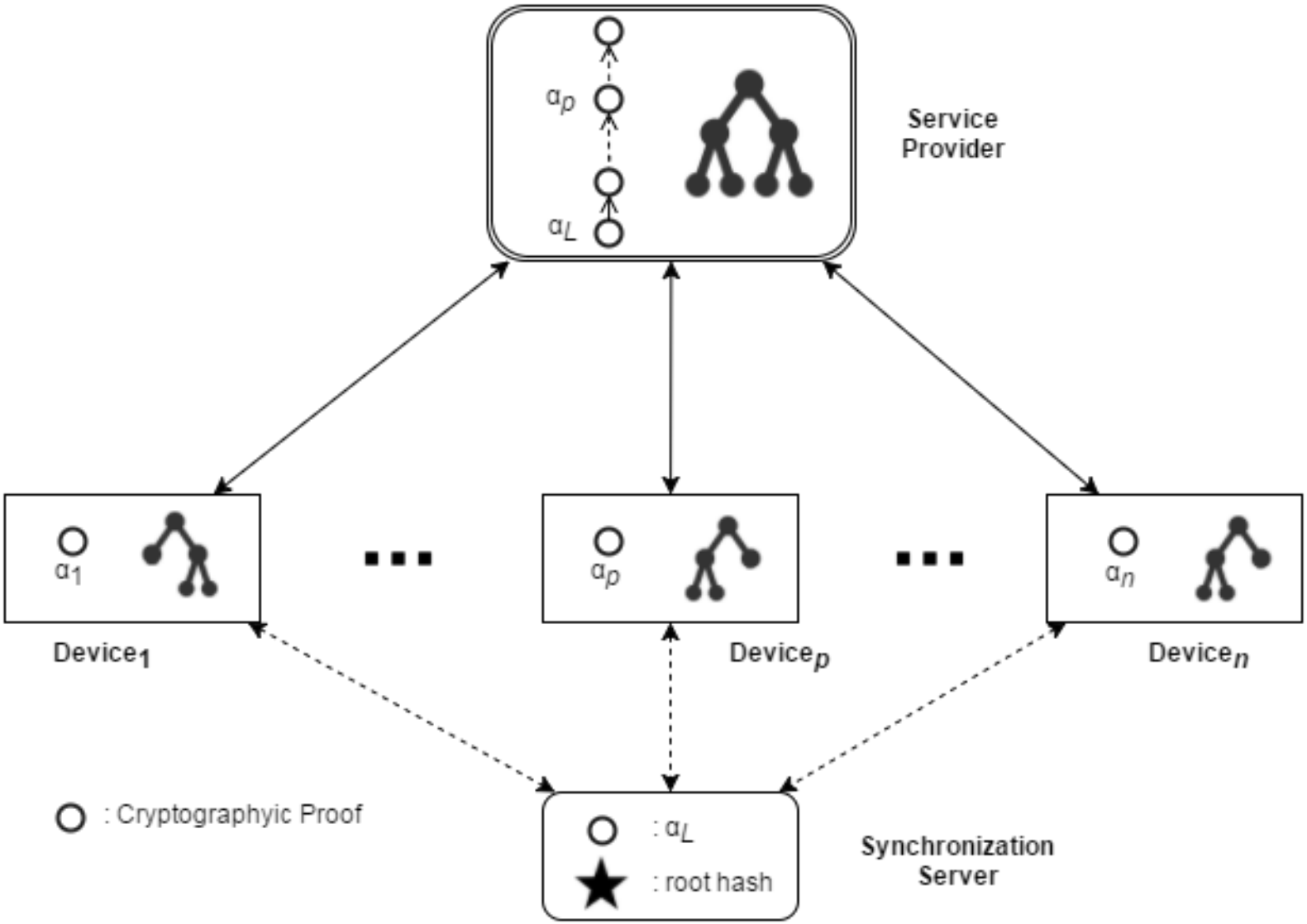
POV - Proof of Violation

定義以下三個 Tuples:

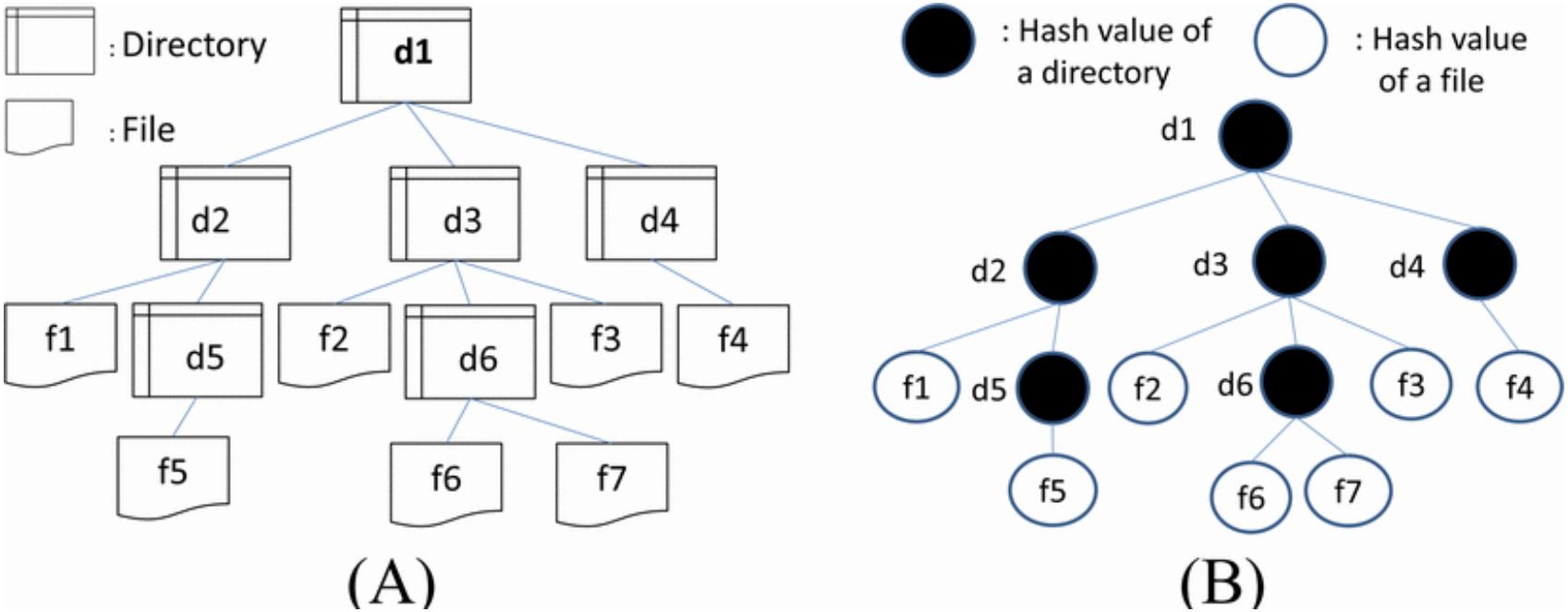
- Properties
  - Data Integrity
  - Write Serializability
  - Read Freshness
- A cryptographic accountability protocol (CAP)
  - 在 User 和 Service Provider 之間交換的訊息加上簽章,
    藉由此 Cryptographic Proof 讓雙方不可否認自己做過的事
- Auditing
  - 利用收集的 Cryptographic Proof 來證明是否違反 Properties

Real-time Proof of Violation for Cloud Storage

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

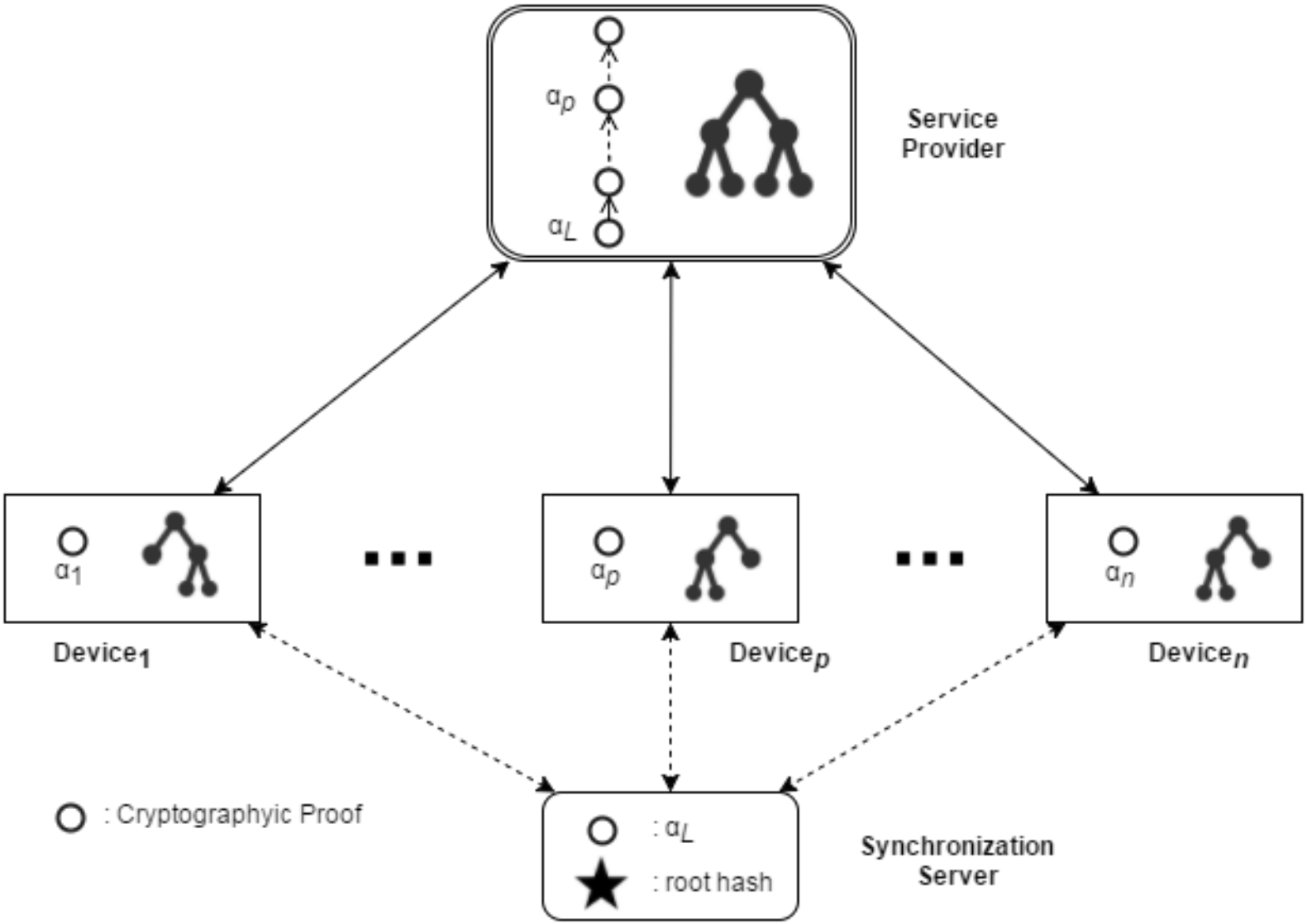


Merkle Tree


: 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)

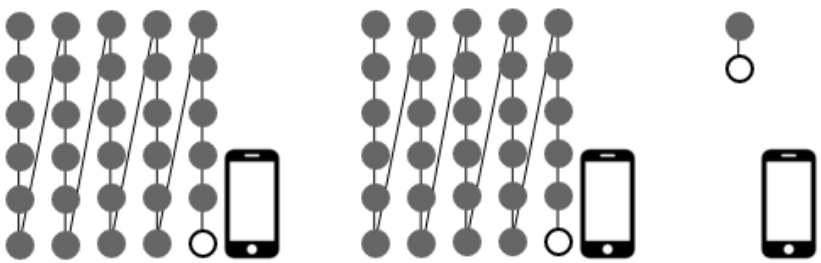
Real-time Proof of Violation for Cloud Storage

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



Worst-case

若有個 device 很久沒有使用，下次要上傳下載檔案前需要花很長的時間將 merkle tree 更新到最新
累積的 hash chain 越長，使用者等待的時間越久

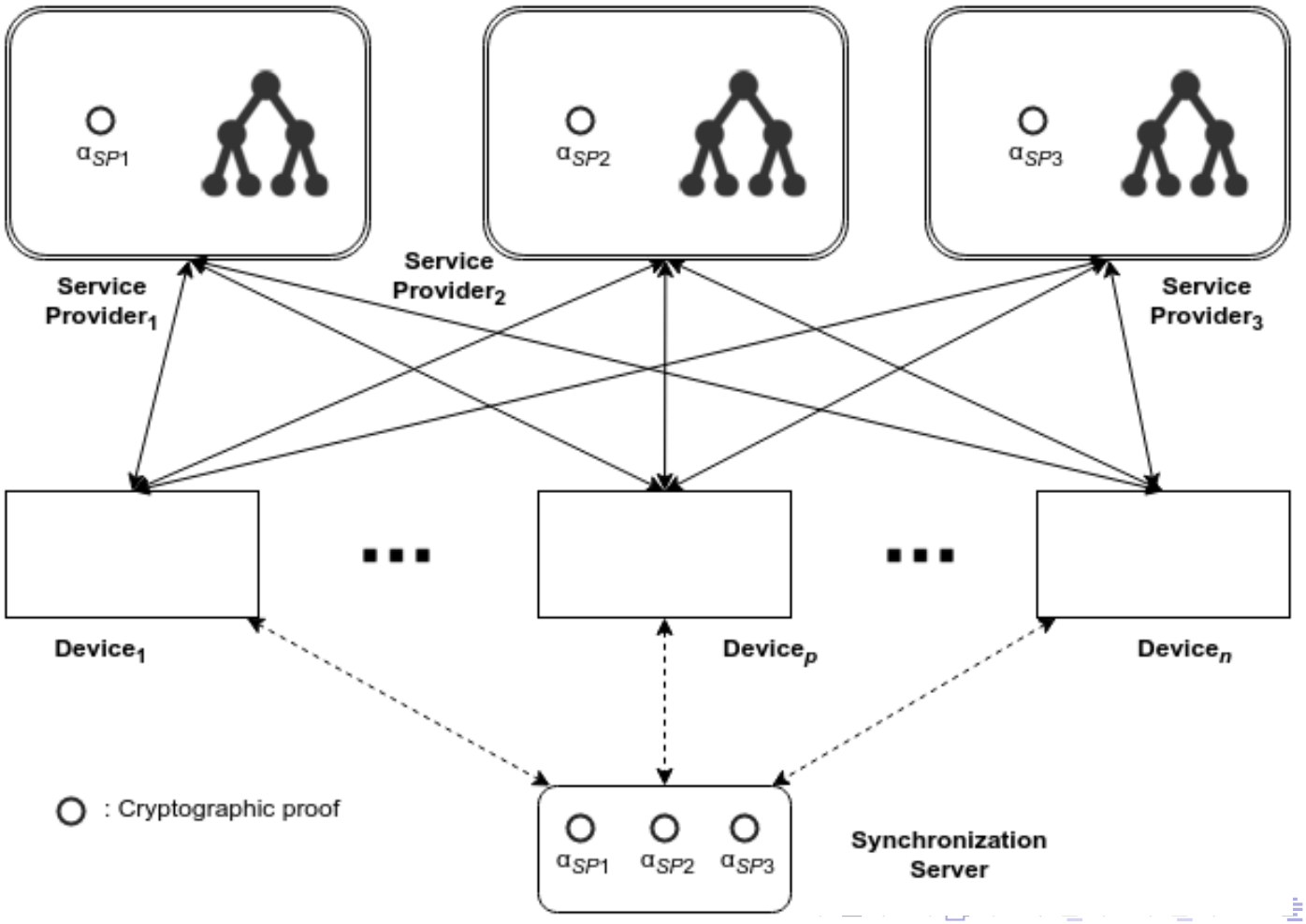


System Architecture

Assumption:

同時 k 個 server，同時回傳相同錯誤結果的機率 ≈ 0

Service Providers are Independent Cloud

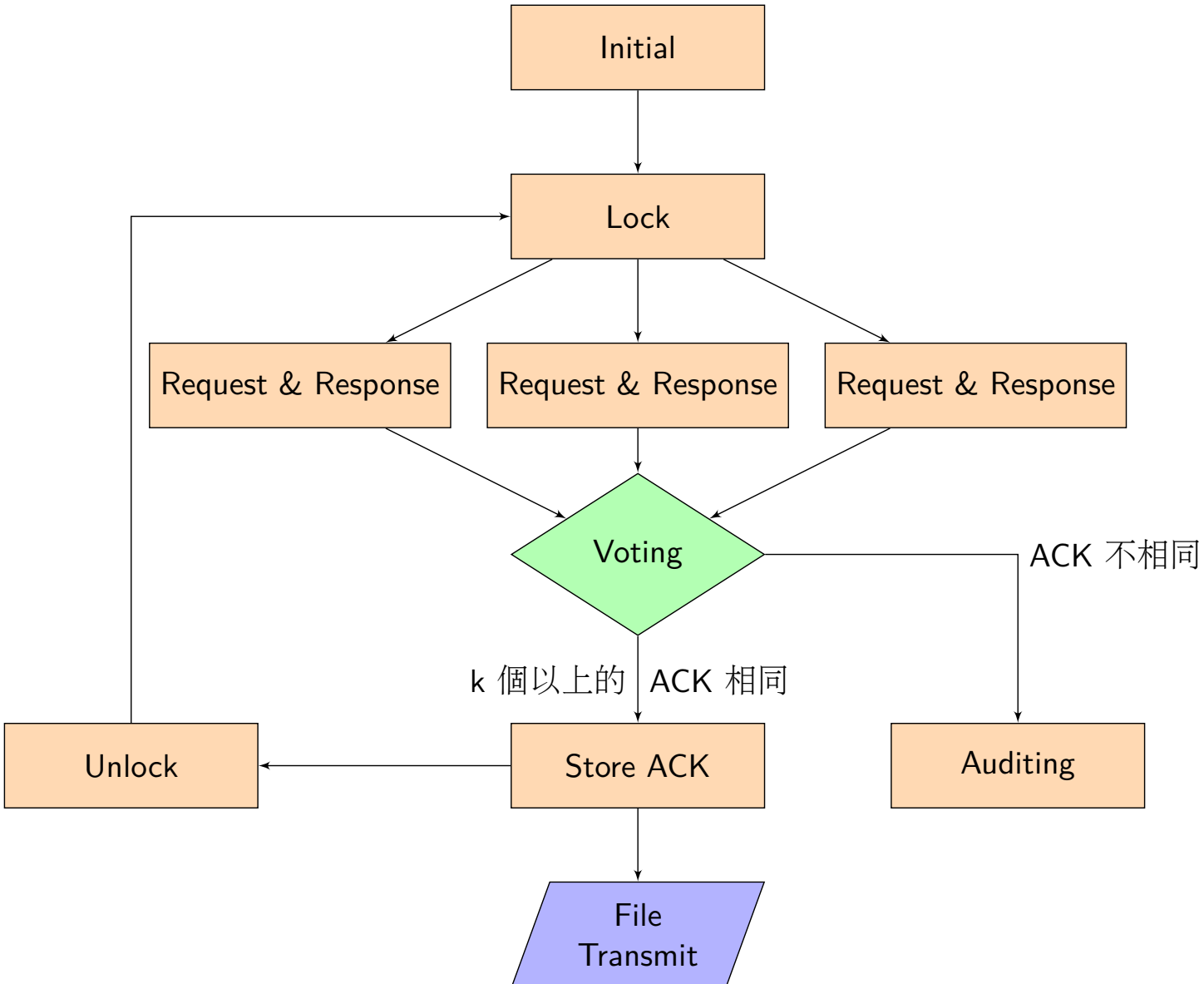


Comparison

- Pros
  1. Device 節省了儲存 Merkle tree 的空間
  2. Device 不需要計算新的 Roothash 將會節省時間
  3. 每一次更新資料都會即時的備份
  4. 不會有之前的 Worst-case

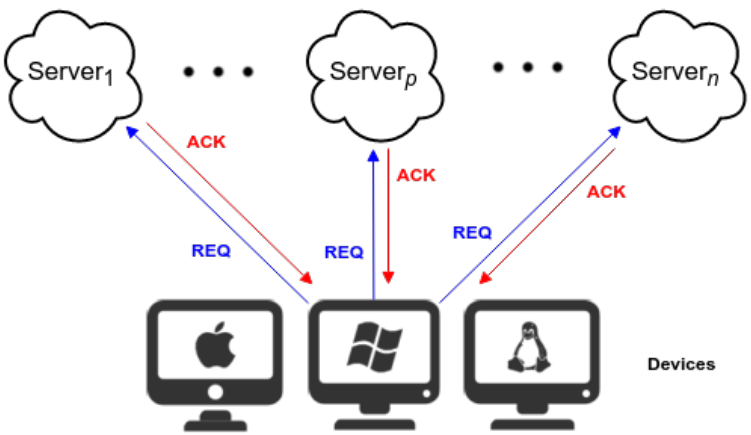
- Cons
  1. 需要傳送多份 Request, 處理多份 Response
  2. 需要使用較多的 Service Provider

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
Auditing
File
Transmit

Download & Upload

Request & Response



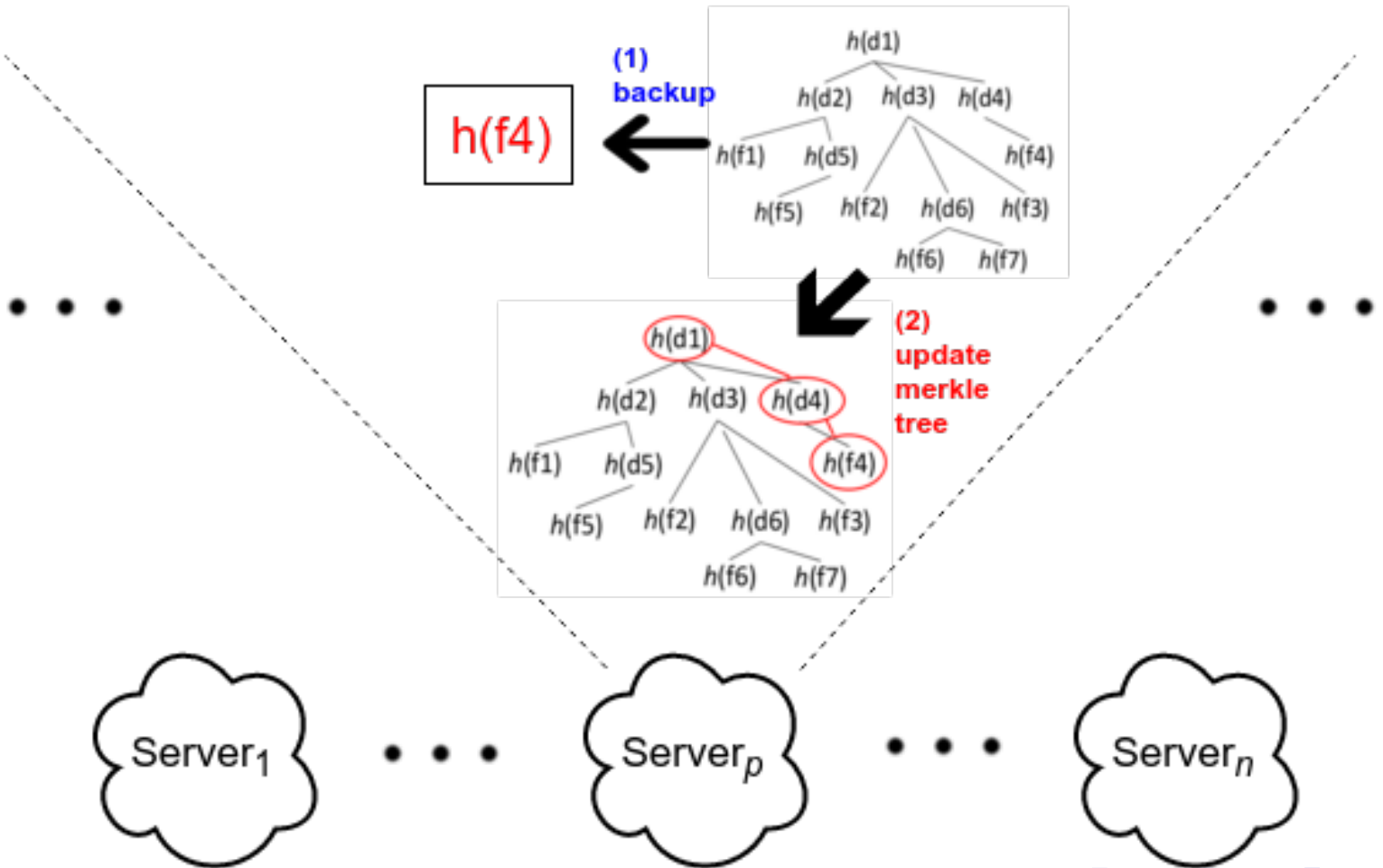
$$REQ = (OP,\ SN,\ [OP,\ SN]_{pri(D)})$$
$$OP = (TYPE,\ PATH,\ HASH)$$
$$SN = Sequence\ Number$$

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

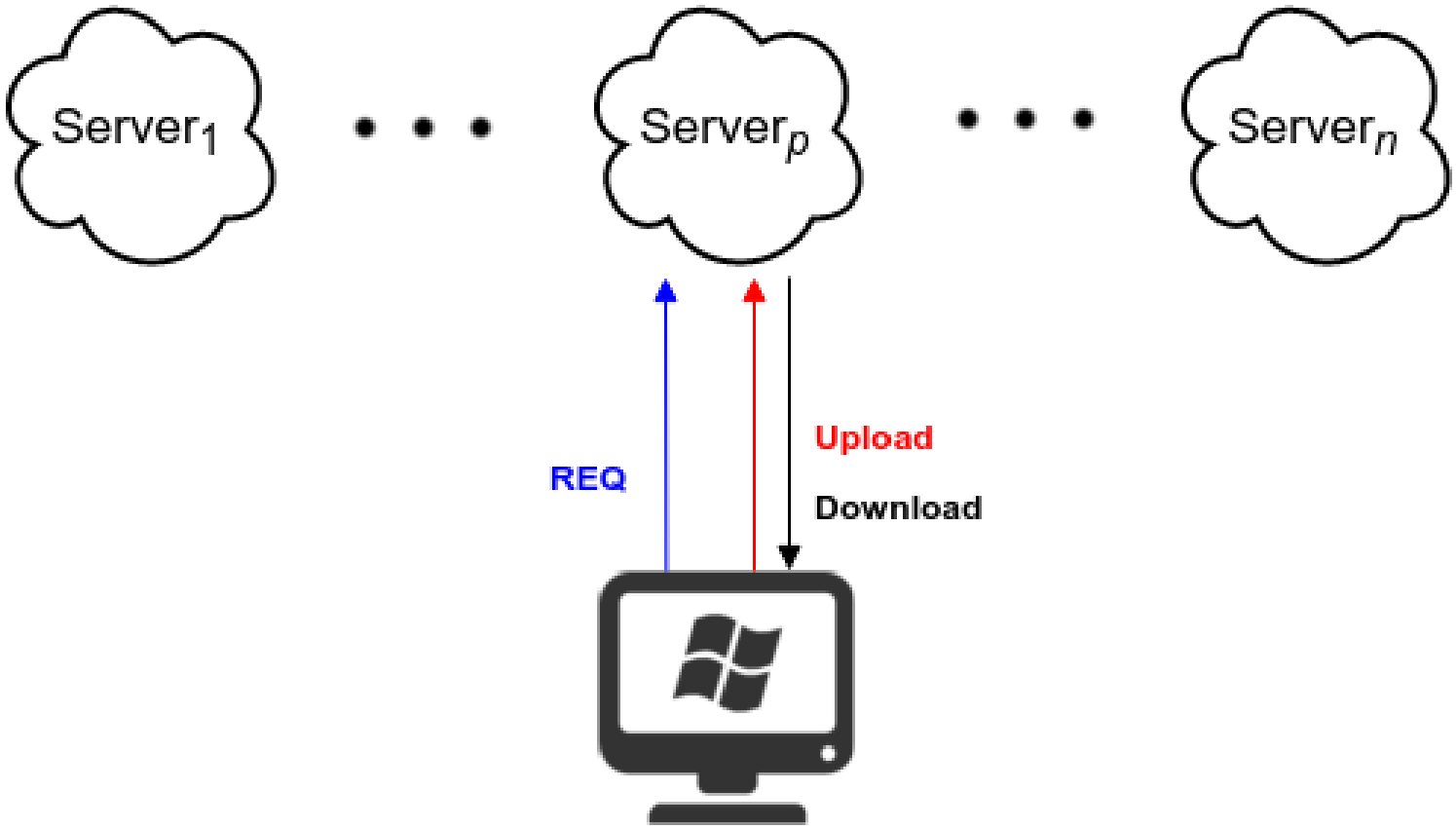
collect ACKs and voting

if Operation is UPLOAD

Servers Update Merkle tree



File Transmit



Audit

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證明 $Server_p$ 出錯

[證明 i 之前的動作都沒問題]

① device 檢查 MT_{i-1} 的 roothash，應和 ACK_{i-1} 中紀錄的相同

[證明第 i 個動作沒問題]

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

Experimental Results

	Size	File	Directory
A	777 MB	48	6
B	145 MB	54198	188
C	5.95 GB	45089	1459

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

	Non Hashed	Pre Hashed	Merkle tree Size
A	9.406	0.003	5.4 KB
B	55.147	2.703	5.08 MB
C	339.181	0.334	4.37 MB

Table: SERIALIZE & DESERIALIZE MERKLE TREE OBJECT'S TIME (IN SEC.)

	Serialize	Deserialize
A	0.040	0.009
B	0.756	0.299
C	0.670	0.295

Outline

Experimental Results
Non POV

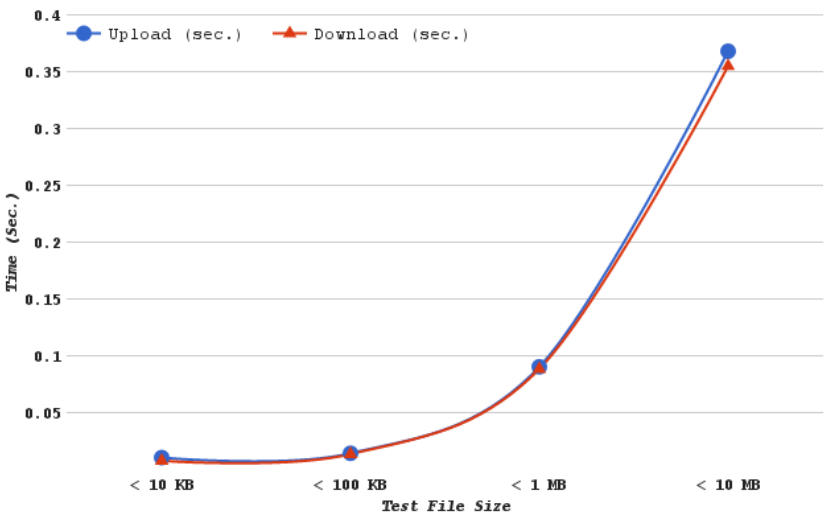
not in the same network segment: from lab to my home (16 hops.)

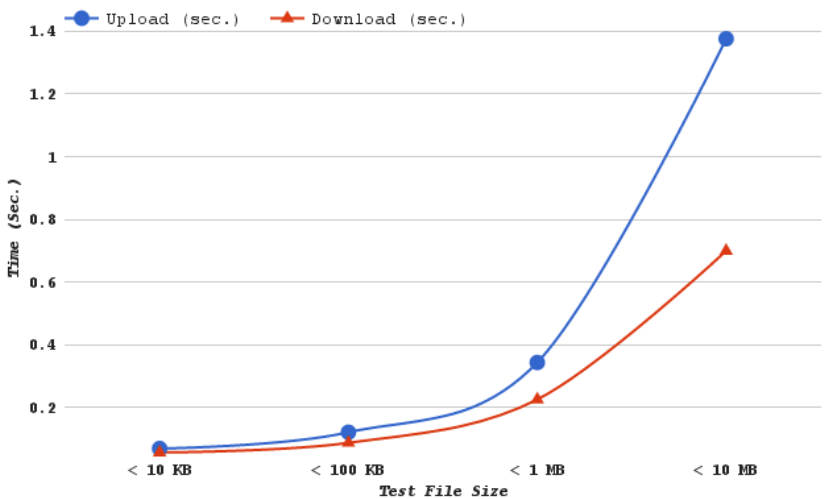
Table: The client device and SP are in the same network segment

	Upload (sec.)	Download (sec.)
<10 KB	0.010	0.007
<100 KB	0.014	0.013
<1 MB	0.090	0.088
<10 MB	0.367	0.354

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

	Upload (sec.)	Download (sec.)
<10 KB	0.069	0.056
<100 KB	0.121	0.087
<1 MB	0.343	0.225
<10 MB	1.675	0.699





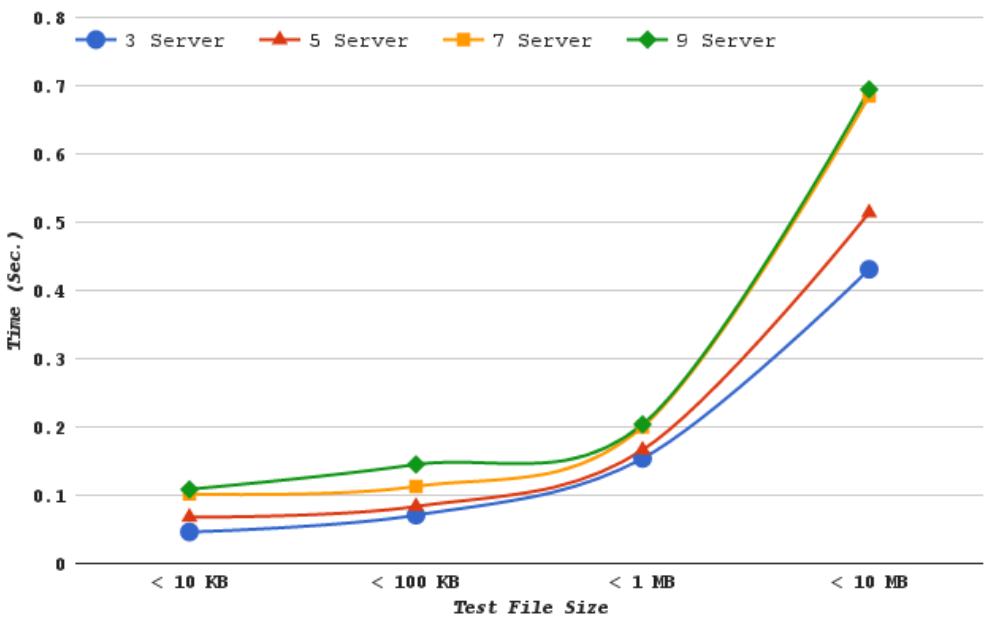
Outline

Experimental Results

The client device and SP are in the same network segment - My Method

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

	3 Server	5 Server	7 Server	9 Server
<10 KB	0.046	0.067	0.101	0.108
<100 KB	0.070	0.083	0.112	0.145
<1 MB	0.153	0.166	0.200	0.203
<10 MB	0.430	0.513	0.684	0.694

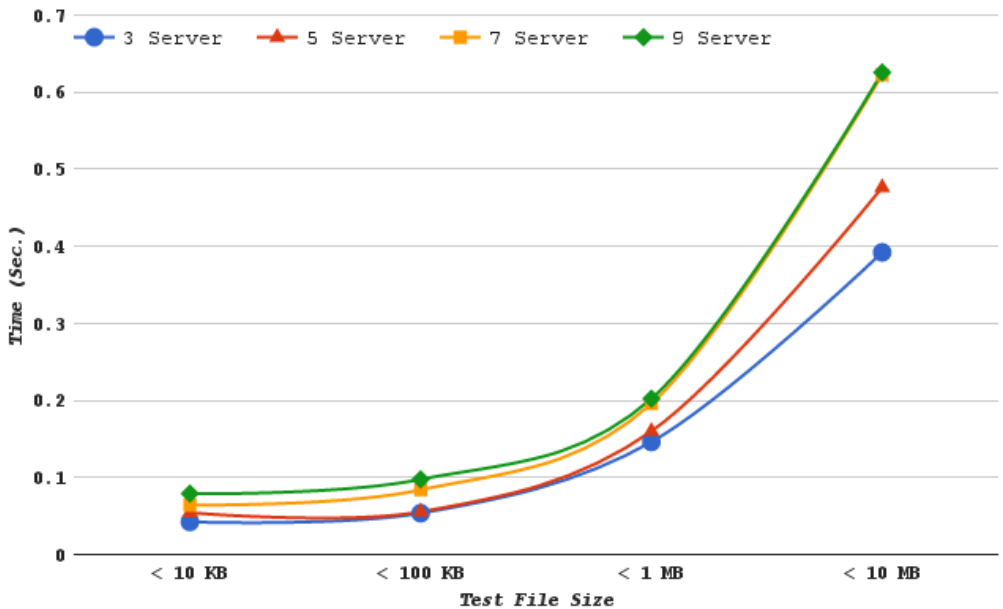


Experimental Results

The client device and SP are in the same network segment - My Method

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

	3 Server	5 Server	7 Server	9 Server
<10 KB	0.042	0.054	0.064	0.078
<100 KB	0.053	0.055	0.083	0.097
<1 MB	0.146	0.159	0.195	0.202
<10 MB	0.392	0.476	0.622	0.625

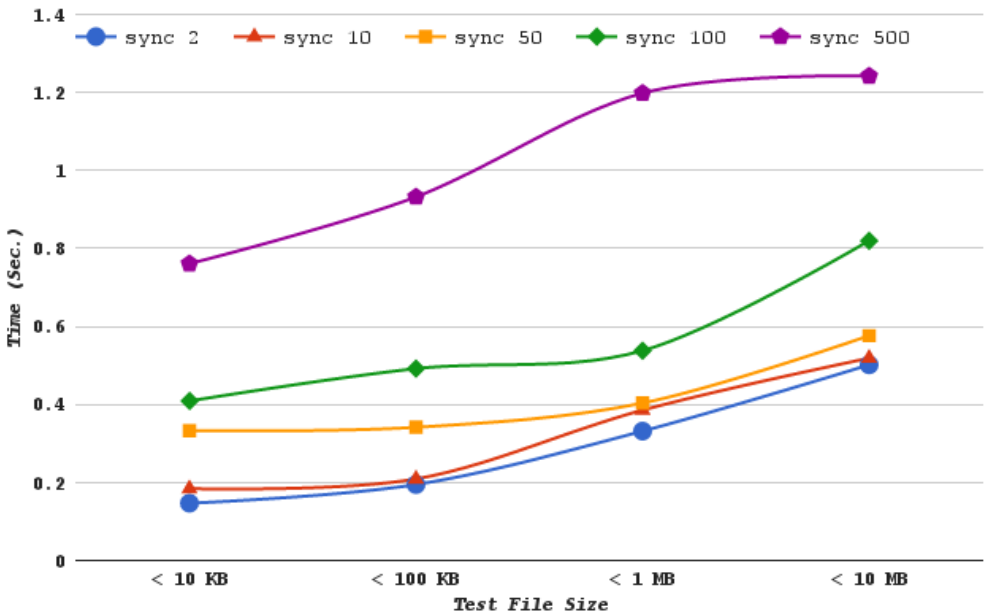


Experimental Results

The client device and SP are in the same network segment - 2014 Cloud Com

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

	sync 2	sync 10	sync 50	sync 100	sync 500
<10 KB	0.146	0.184	0.332	0.409	0.760
<100 KB	0.194	0.209	0.341	0.491	0.932
<1 MB	0.331	0.385	0.403	0.537	1.198
<10 MB	0.501	0.518	0.576	0.819	1.242

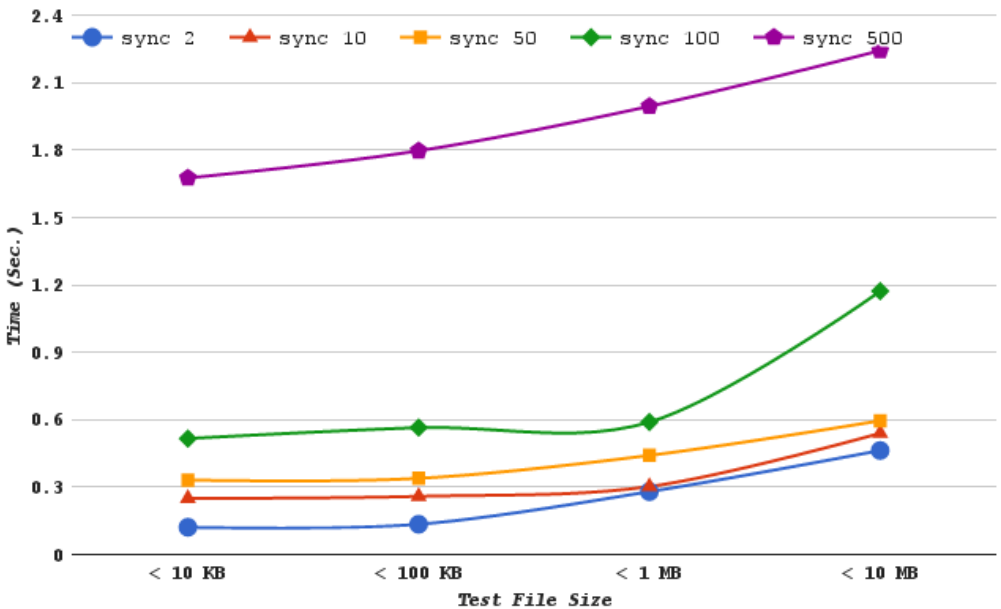


Experimental Results

The client device and SP are in the same network segment - 2014 Cloud Com

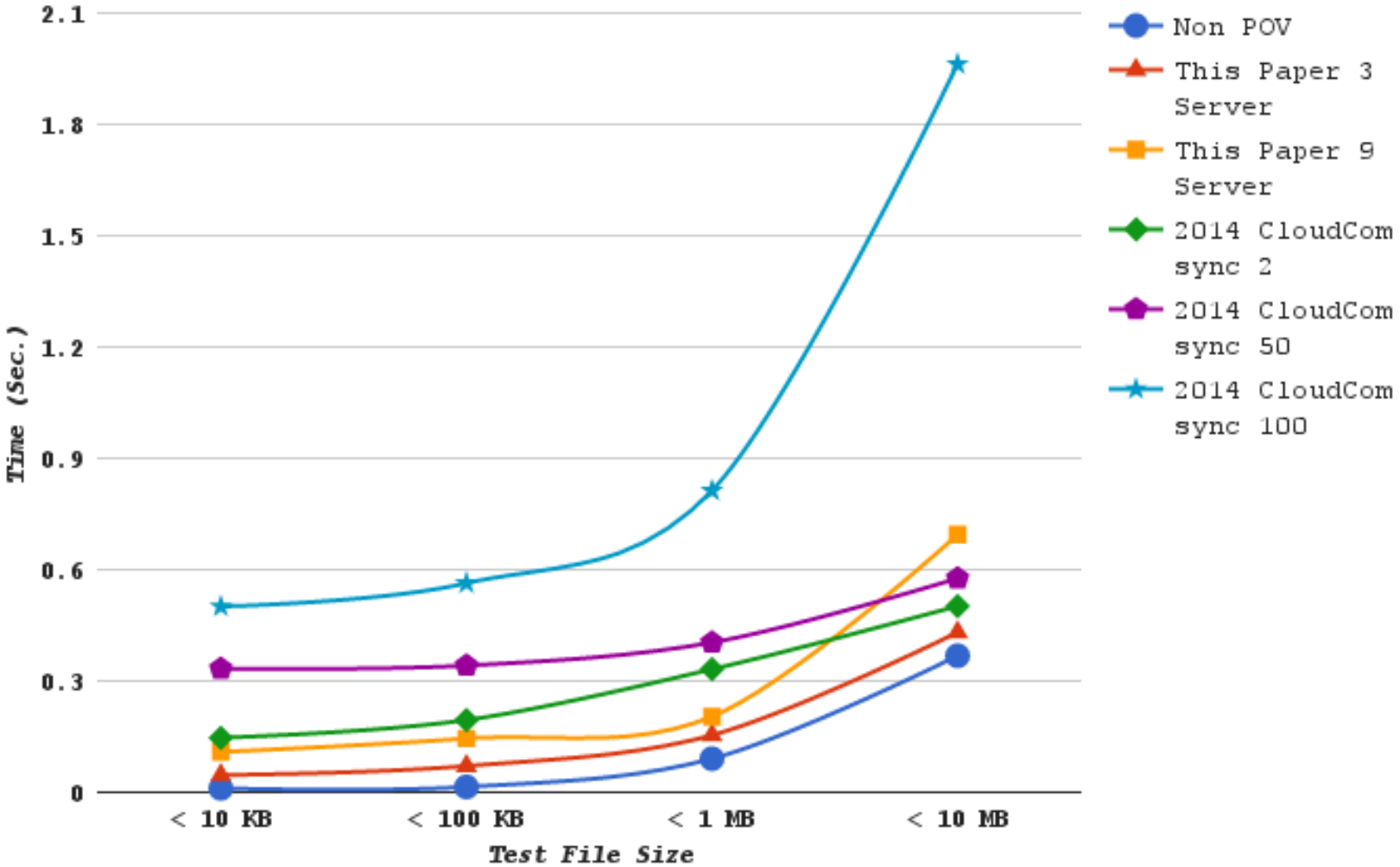
Table: THE EXECUTION TIME OF DOWNLOAD OPERATIONS (IN SEC.) (Account C)

	sync 2	sync 10	sync 50	sync 100	sync 500
<10 KB	0.121	0.249	0.331	0.515	1.675
<100 KB	0.134	0.258	0.338	0.564	1.796
<1 MB	0.279	0.302	0.440	0.588	1.994
<10 MB	0.462	0.539	0.595	1.171	2.241



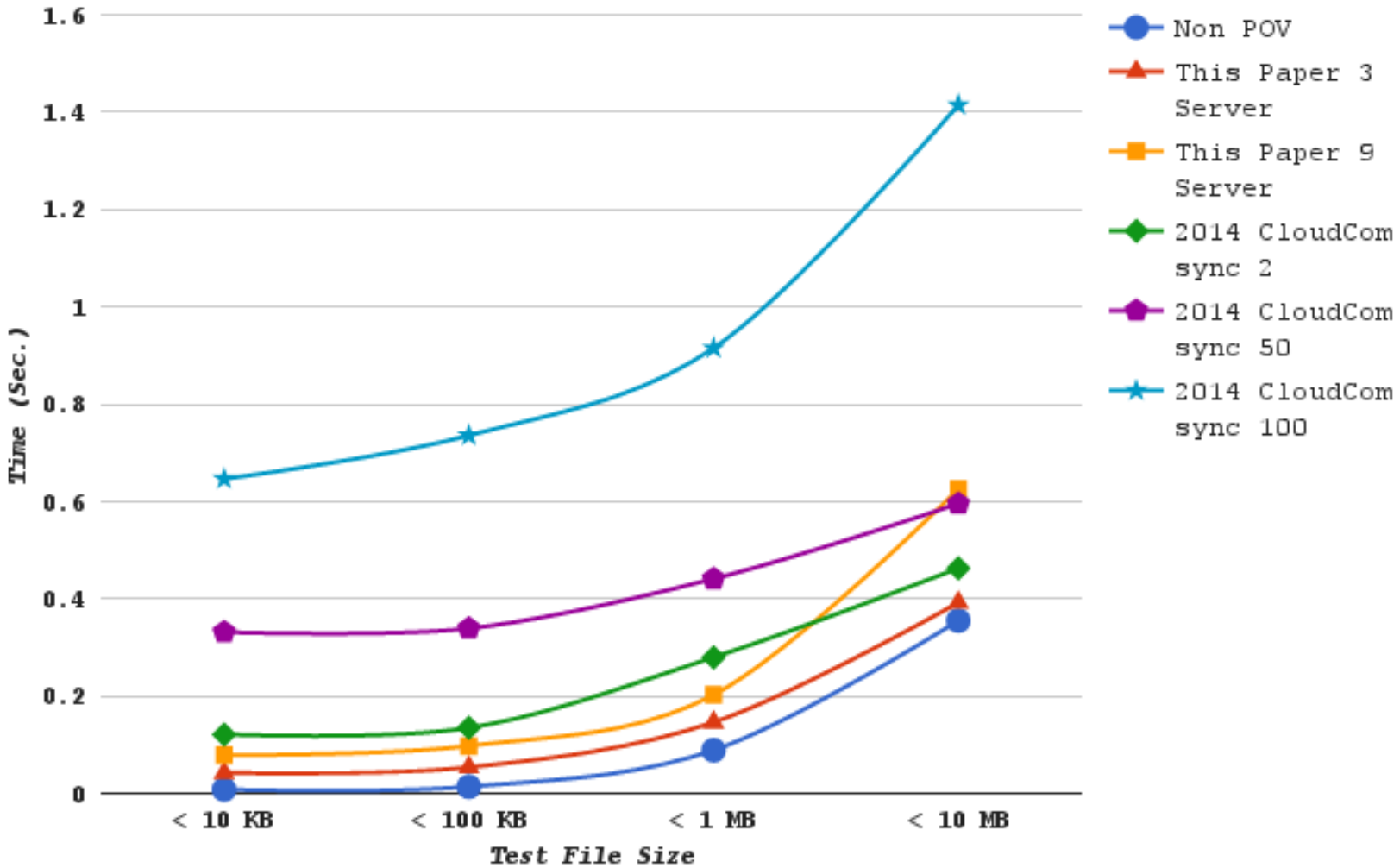
Experimental Results

The client device and SP are in the same network segment - UPLOAD operation



Experimental Results

The client device and SP are in the same network segment - DOWNLOAD operation



Experimental Results

The client device and SP are in the same network segment - UPLOAD Overhead

Table: My Method / Non POV (IN SEC.) (Account C)

	3 Server	5 Server	7 Server	9 Server
<10 KB	4.349	6.403	9.584	10.246
<100 KB	4.914	5.805	7.843	10.077
<1 MB	1.700	1.838	2.211	2.254
<10 MB	1.171	1.396	1.860	1.886

Table: 2014 Cloud Com / Non POV (IN SEC.) (Account C)

	sync 2	sync 10	sync 50	sync 100	sync 500
<10 KB	13.837	17.358	31.390	38.556	71.722
<100 KB	13.523	14.524	23.720	34.181	64.759
<1 MB	3.666	4.262	4.461	5.947	13.247
<10 MB	1.363	1.409	1.566	2.228	3.375

Avg: 3.97 times, Max: 6.99 times

Experimental Results

The client device and SP are in the same network segment - DOWNLOAD Overhead

Table: My Method / Non POV (IN SEC.) (Account C)

	3 Server	5 Server	7 Server	9 Server
<10 KB	5.391	6.917	8.205	10.054
<100 KB	3.913	4.049	6.132	7.121
<1 MB	1.648	1.805	2.210	2.283
<10 MB	1.104	1.341	1.754	1.762

Table: 2014 Cloud Com / Non POV (IN SEC.) (Account C)

	sync 2	sync 10	sync 50	sync 250	sync 1250
<10 KB	15.459	31.844	42.238	119.489	532.253
<100 KB	9.828	18.896	24.745	70.345	307.573
<1 MB	3.156	3.412	4.977	13.265	48.482
<10 MB	1.303	1.520	1.676	3.514	12.286

Avg: 7.91 times, Max: 21.24 times

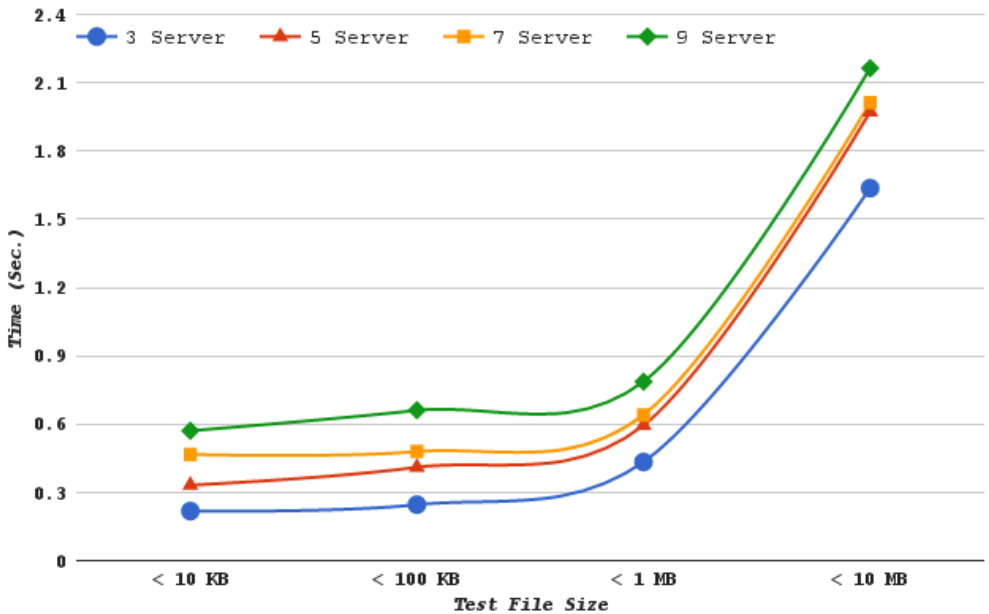
Outline

Experimental Results

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

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

	3 Server	5 Server	7 Server	9 Server
<10 KB	0.217	0.331	0.466	0.570
<100 KB	0.245	0.410	0.479	0.660
<1 MB	0.433	0.594	0.640	0.786
<10 MB	1.636	1.972	2.011	2.163

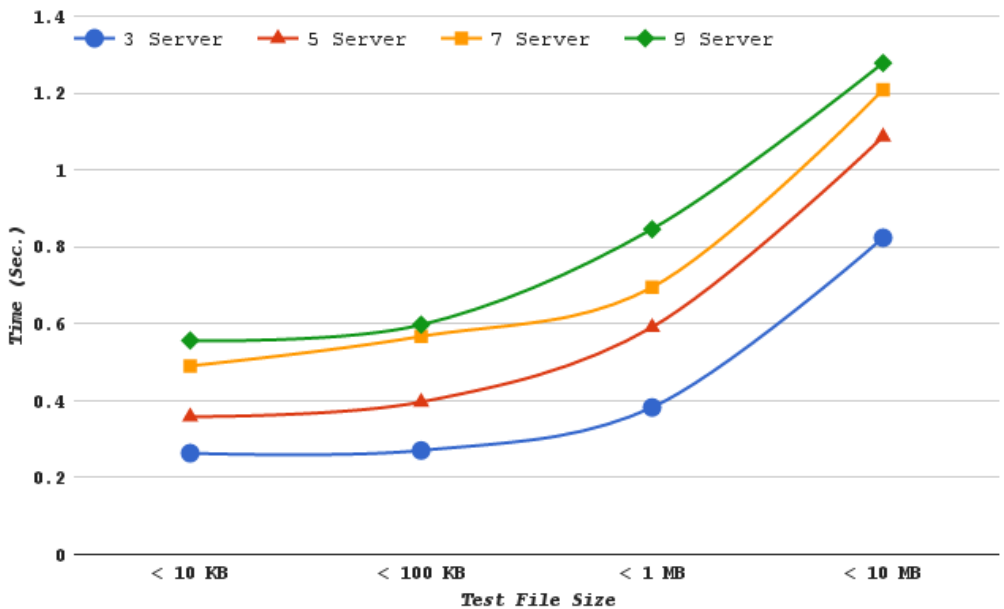


Experimental Results

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

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

	3 Server	5 Server	7 Server	9 Server
<10 KB	0.263	0.358	0.490	0.556
<100 KB	0.270	0.396	0.567	0.597
<1 MB	0.382	0.590	0.694	0.846
<10 MB	0.823	1.086	1.208	1.278

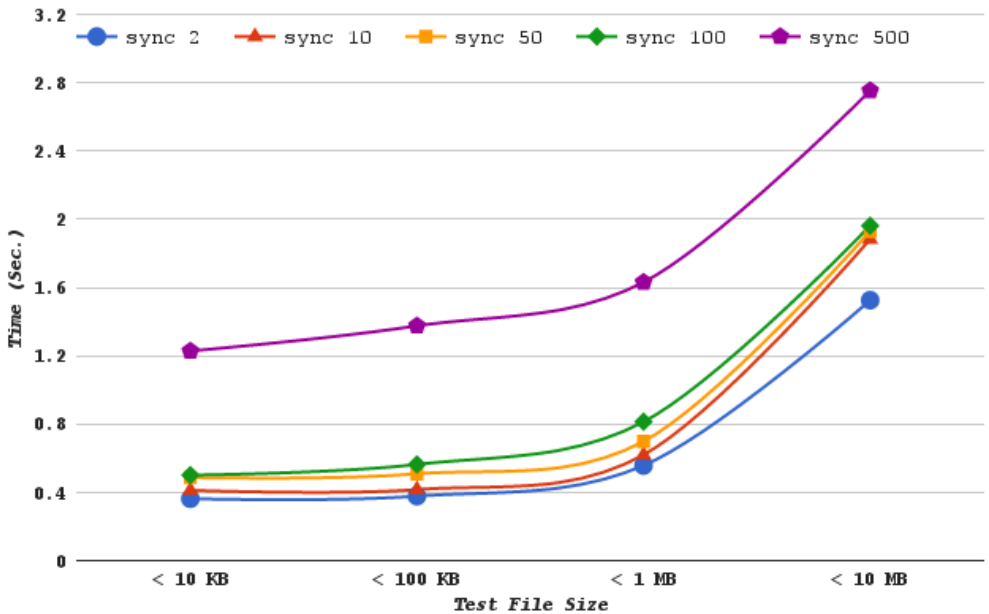


Experimental Results

The client device and SP are not in the same network segment - 2014 Cloud Com

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

	sync 2	sync 10	sync 50	sync 100	sync 500
<10 KB	0.362	0.411	0.486	0.500	1.227
<100 KB	0.377	0.416	0.508	0.563	1.375
<1 MB	0.556	0.619	0.698	0.812	1.630
<10 MB	1.525	1.882	1.929	1.962	2.753

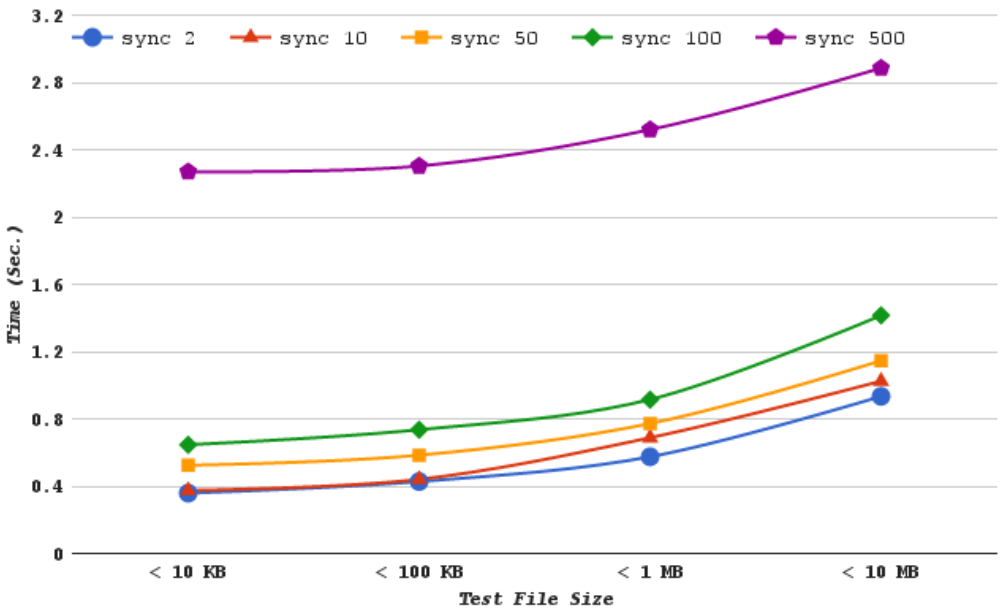


Experimental Results

The client device and SP are not in the same network segment - 2014 Cloud Com

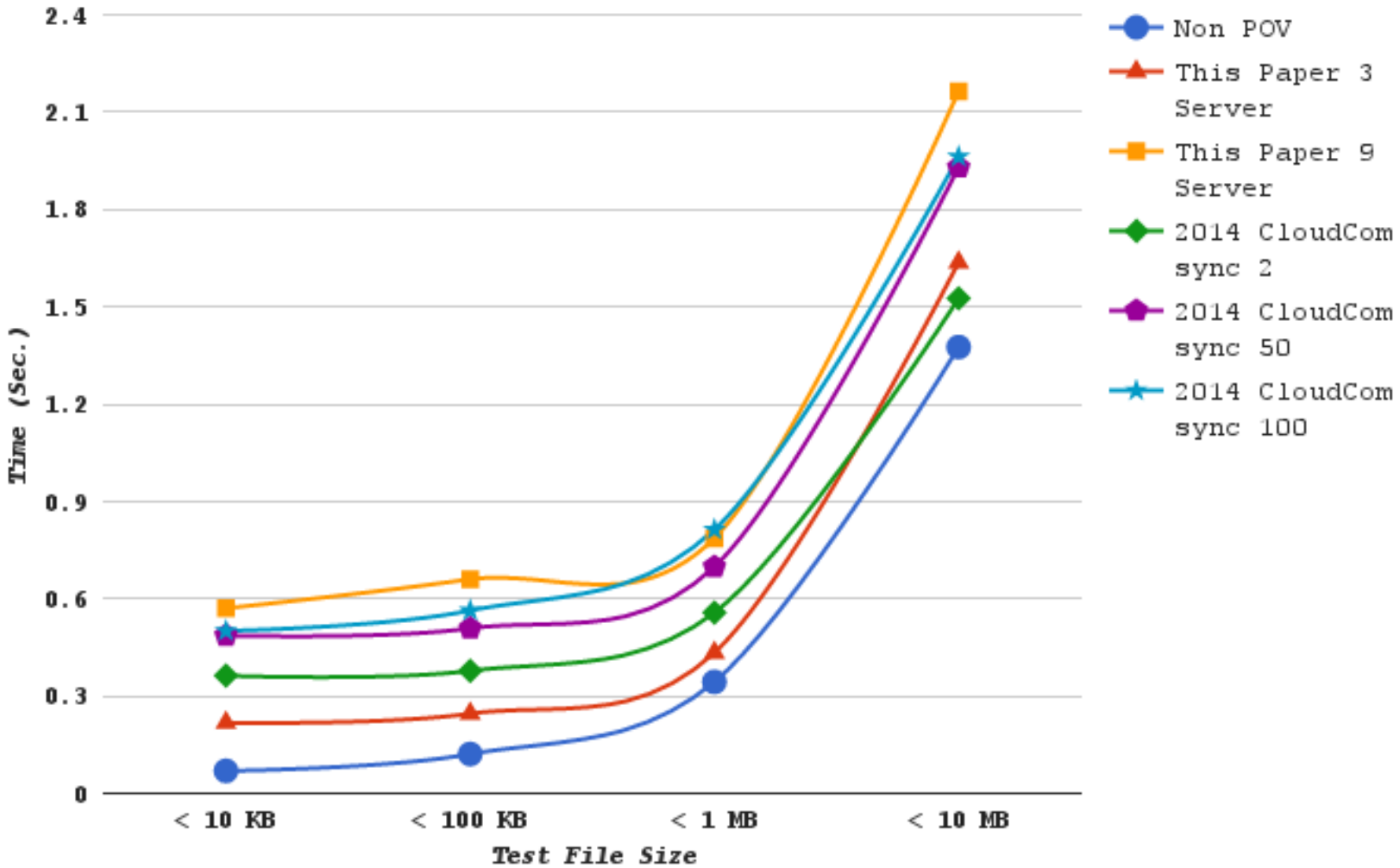
Table: THE EXECUTION TIME OF DOWNLOAD OPERATIONS (IN SEC.) (Account C)

	sync 2	sync 10	sync 50	sync 100	sync 500
<10 KB	0.388	0.374	0.524	0.646	2.269
<100 KB	0.427	0.440	0.584	0.735	2.302
<1 MB	0.574	0.687	0.772	0.914	2.519
<10 MB	0.933	1.024	1.145	1.414	2.884



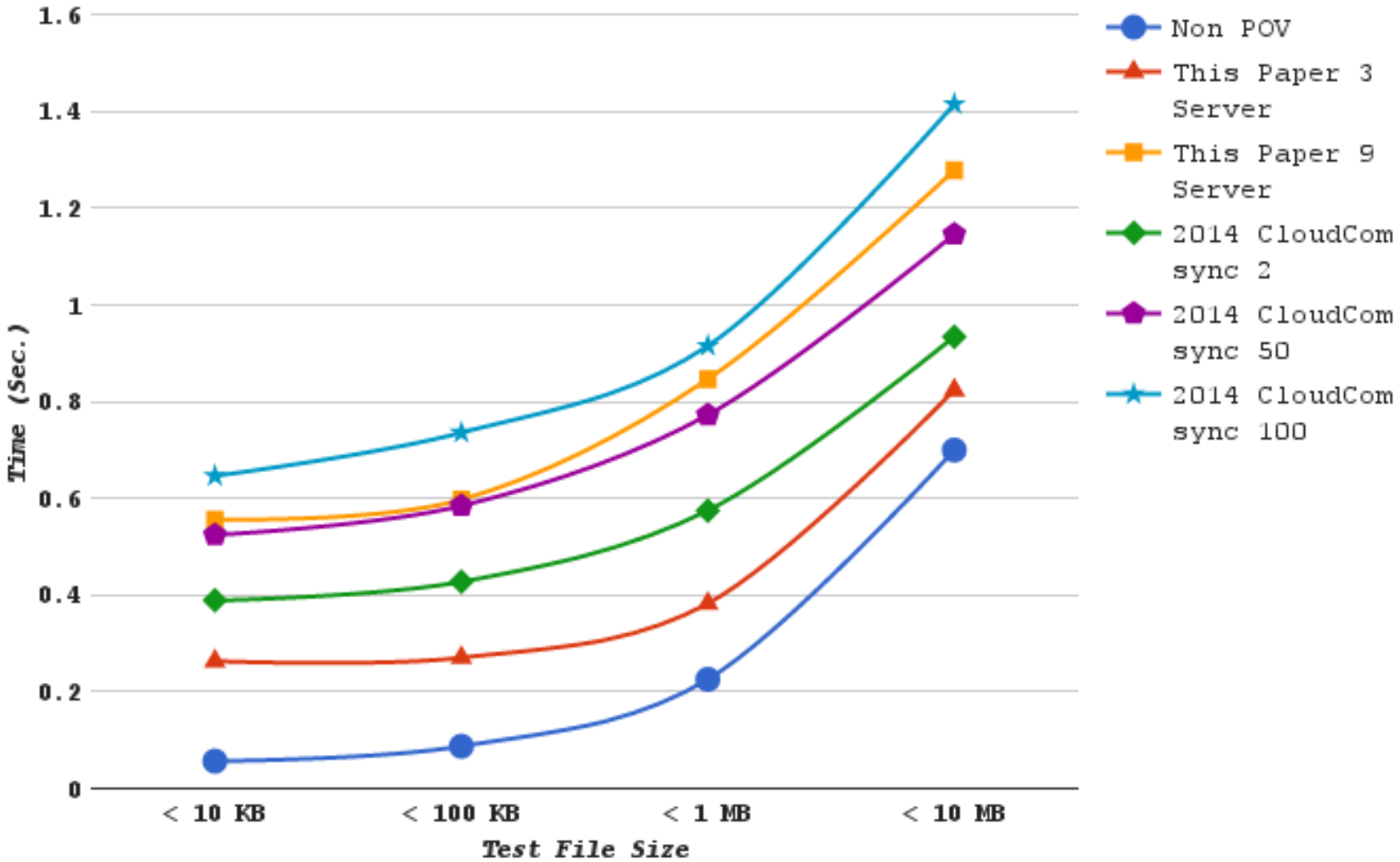
Experimental Results

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



Experimental Results

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



Experimental Results

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

Table: My Method / Non POV (IN SEC.) (Account C)

	3 Server	5 Server	7 Server	9 Server
<10 KB	3.140	4.783	6.736	8.234
<100 KB	2.029	3.387	3.957	5.451
<1 MB	1.261	1.730	1.864	2.289
<10 MB	1.189	1.433	1.462	1.573

Table: 2014 Cloud Com / Non POV (IN SEC.) (Account C)

	sync 2	sync 10	sync 50	sync 100	sync 500
<10 KB	5.236	5.946	7.023	7.229	17.722
<100 KB	3.119	3.438	4.201	4.653	11.357
<1 MB	1.620	1.802	2.032	2.365	4.746
<10 MB	1.108	1.368	1.402	1.426	2.001

Avg: 1.42 times, Max: 2.15 times

Experimental Results

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

Table: My Method / Non POV (IN SEC.) (Account C)

	3 Server	5 Server	7 Server	9 Server
<10 KB	4.650	6.329	8.658	9.820
<100 KB	3.095	4.539	6.491	6.835
<1 MB	1.694	2.620	3.079	3.751
<10 MB	1.177	1.553	1.727	1.827

Table: 2014 Cloud Com / Non POV (IN SEC.) (Account C)

	sync 2	sync 10	sync 50	sync 100	sync 500
<10 KB	6.860	6.608	9.254	11.410	40.073
<100 KB	4.890	5.041	6.687	8.419	26.364
<1 MB	2.547	3.049	3.423	4.056	11.168
<10 MB	1.335	1.464	1.637	2.022	4.124

Avg: 1.88 times, Max: 4.08 times

Conclusion

我們提出了一個應用於雲端儲存的 Real-time POV 技術，利用投票的方式快速檢查 Data Integrity，也即時的將資料備份到多個 Server 上。

實驗結果顯示，相較於之前的 Real-time POV 技術，平均能夠節省 8 倍的時間，Worst-case 時更能夠節省超過 20 倍的時間。

雲端儲存系統可以使用本論文提出的方法，提供雙方不可否認的保證於他們的服務層級協議 (Service Level Agreement) 中。

Future Work

1. 我們希望能將 FBHTree[1]套用到本論文的方法中，藉由實驗觀察能否增快 Merkle tree 在更新檔案時的速度。

2. 在本論文中使用同步伺服器來維護 Write Serializability，若有新的演算法能夠不需依賴同步伺服器又能維護 Write Serializability，將能讓我們的架構更加彈性且使用更少的硬體。

[1] G.-H. Hwang and H.-F. Chen, "Efficient Real-time Auditing and Proof of Violation for Cloud Storage Systems," in 9th IEEE International Conference on Cloud Computing, San Francisco, USA, 2016.

Thanks for Your Listening