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

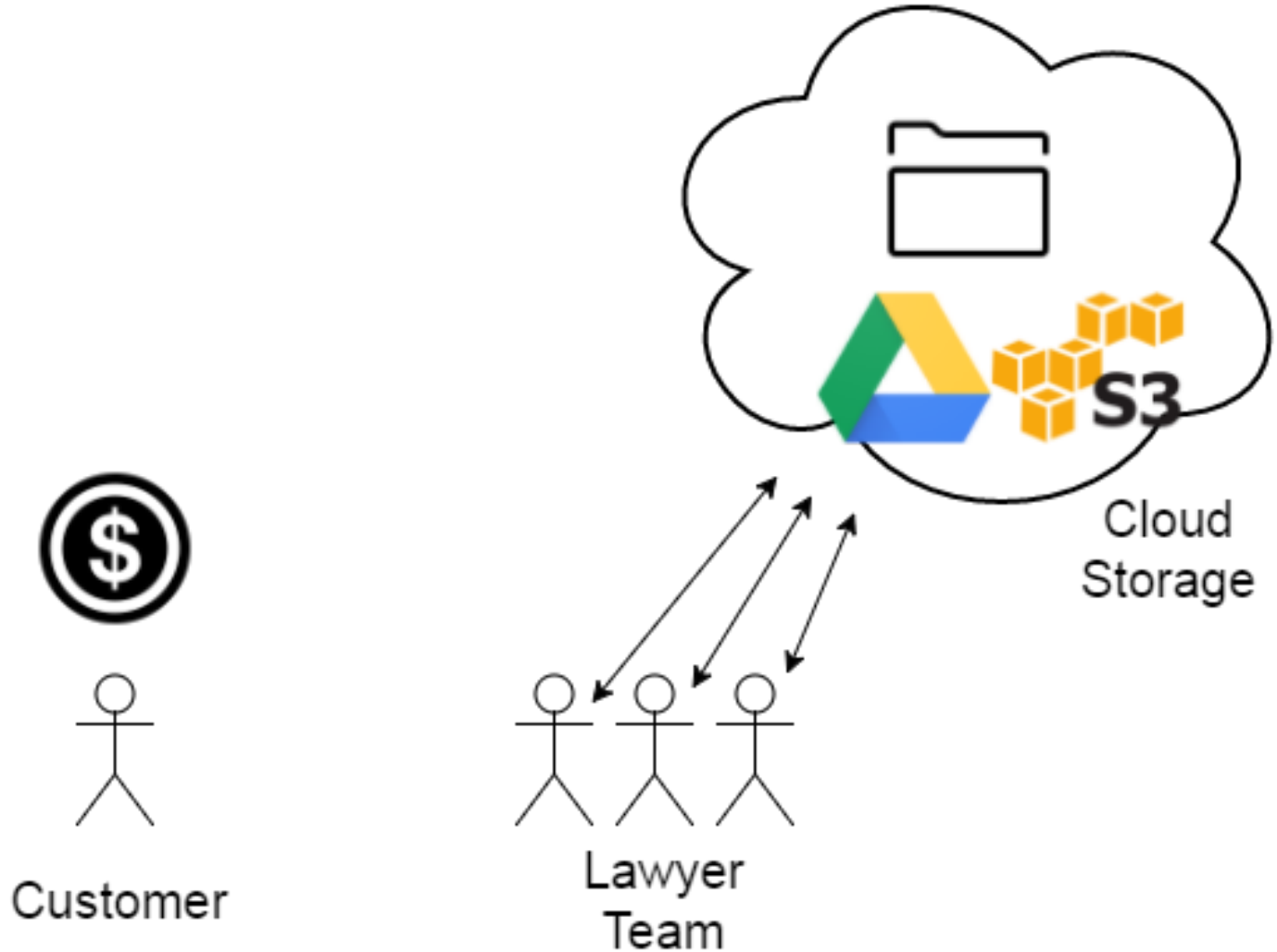
Advicer : Gwan-Hwan Hwang
Student : Wei-Chih Chien

NTNU CSIE CCLAB

2016.07

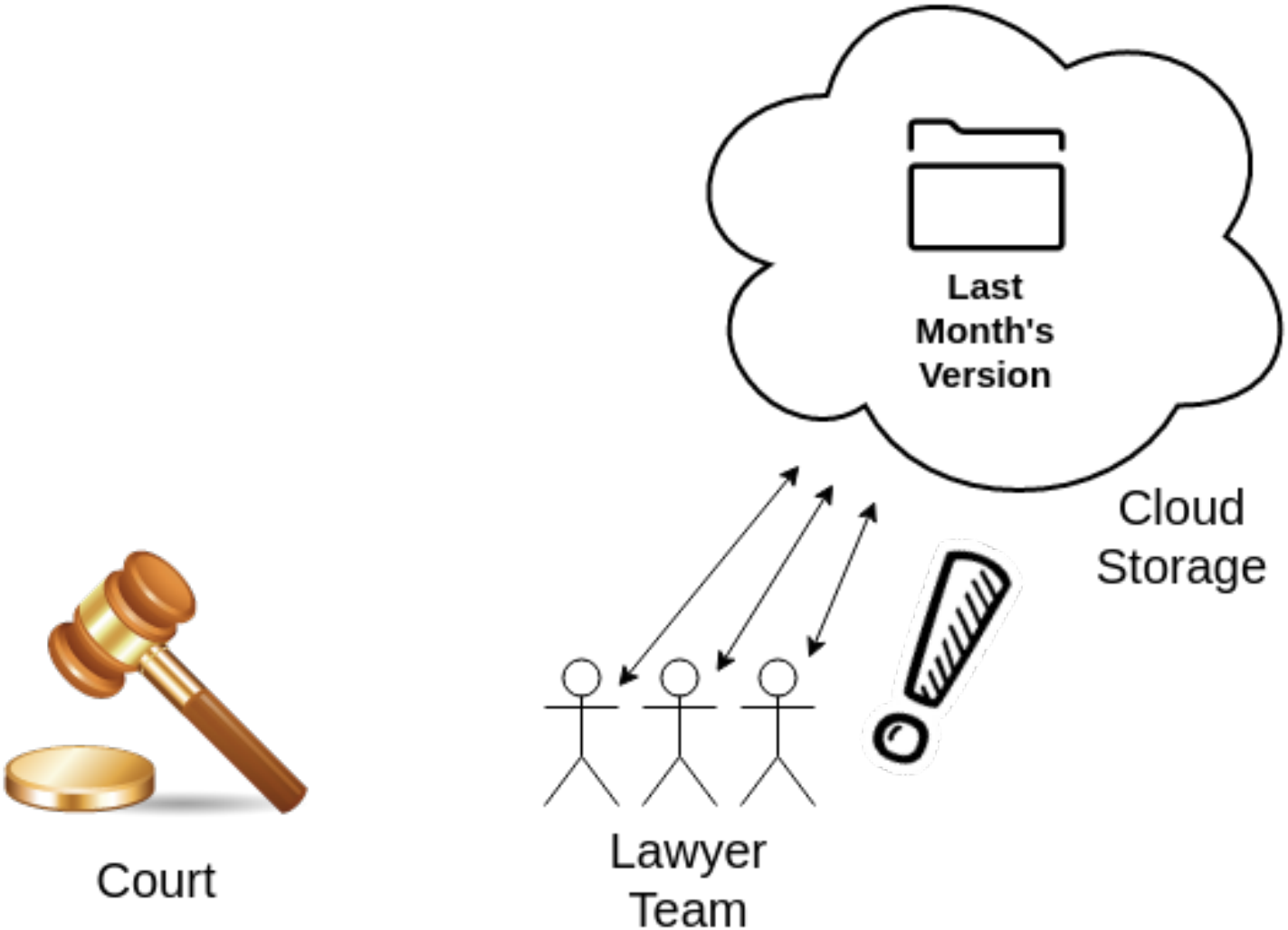
Outline

Scenario
Law Office



Scenario (CON'T)

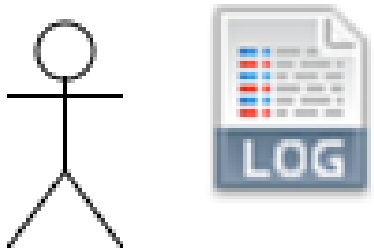
What if...



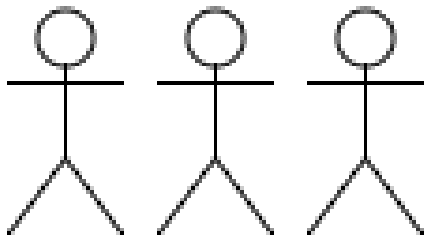
Scenario (CON'T)

No Error !

No Evidence ...

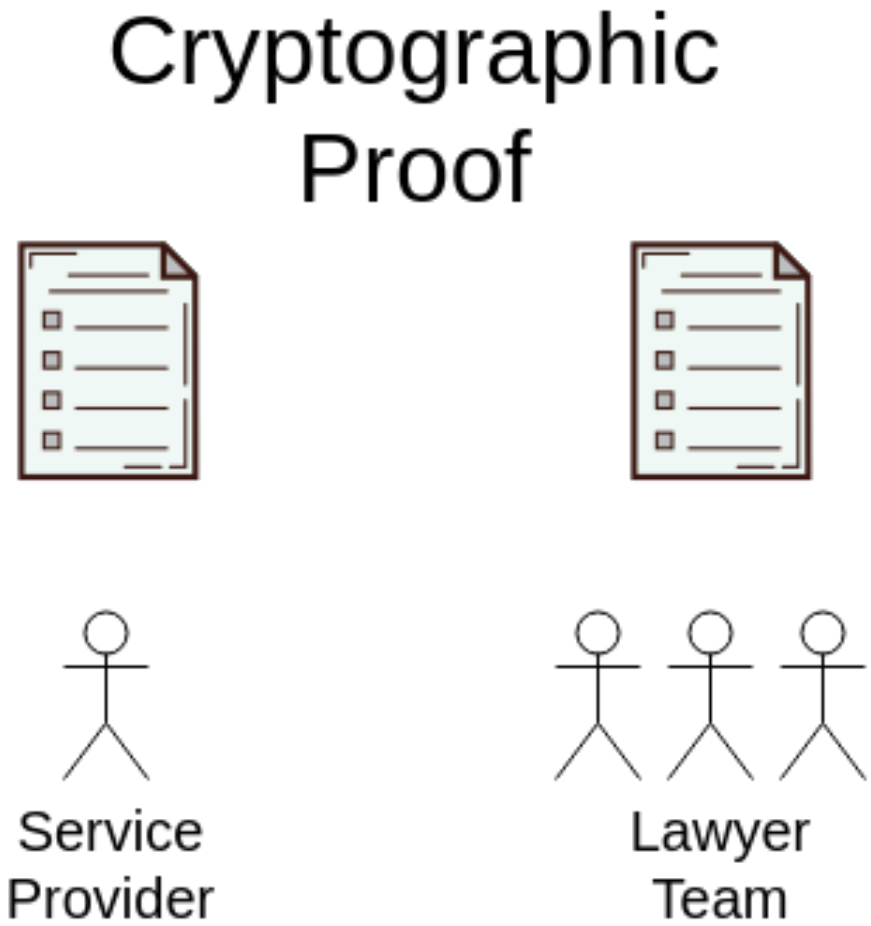


Service Provider



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.

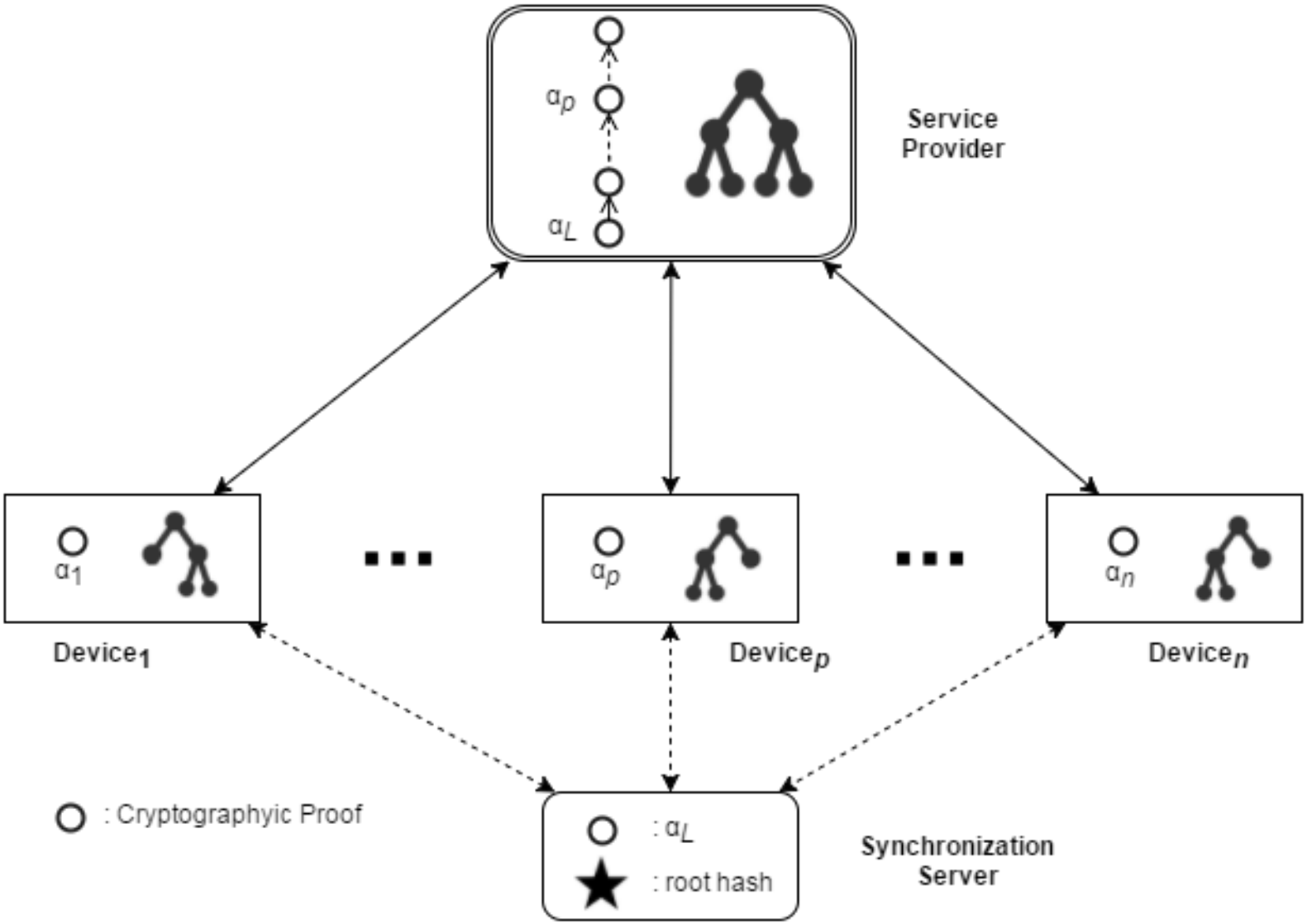
POV - Proof of Violation

定義以下三個 Tuples:

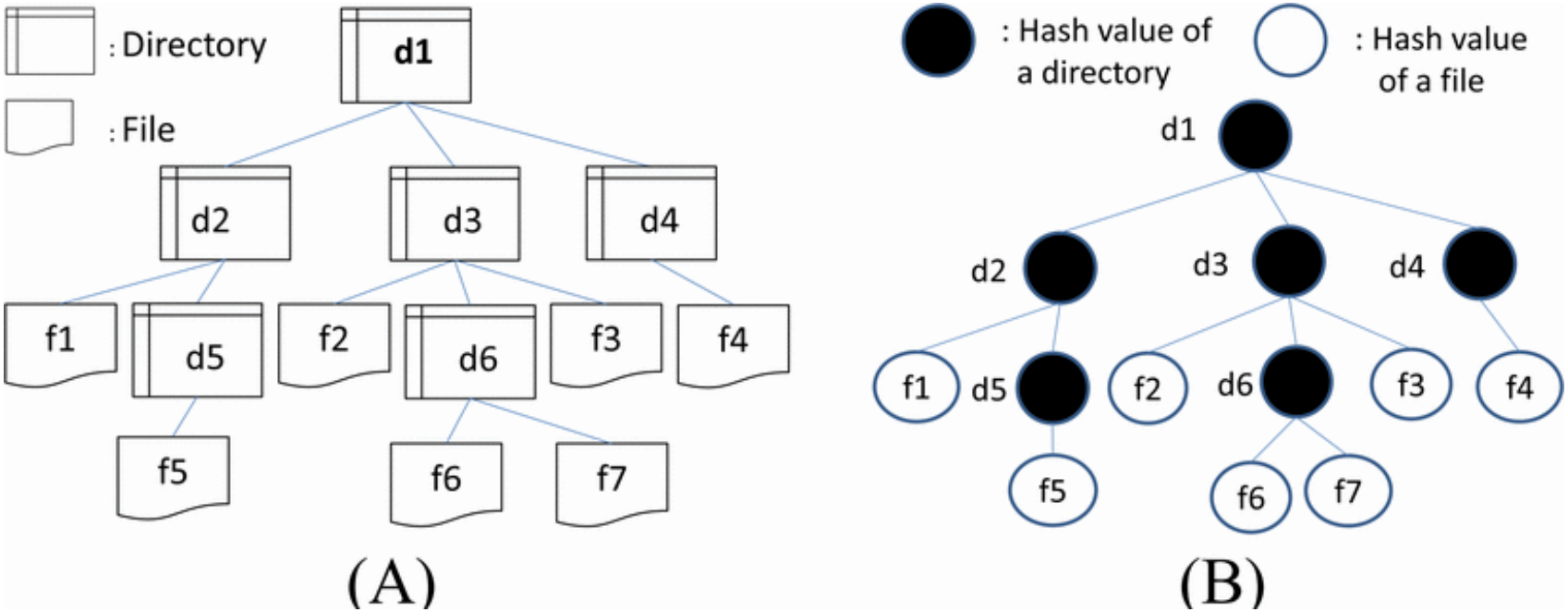
- Properties
  - Data Integrity
  - Write Serializability
  - Read Freshness
- A cryptographic accountability protocol (CAP)
  - 在 User 和 Service Provider 之間交換的訊息加上簽章,
    藉由此 Cryptographic Proof 讓雙方不可否認自己做過的事
- Auditing
  - 利用收集的 Cryptographic Proof 來證明是否違反 Properties

Real-time Proof of Violation for Cloud Storage

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

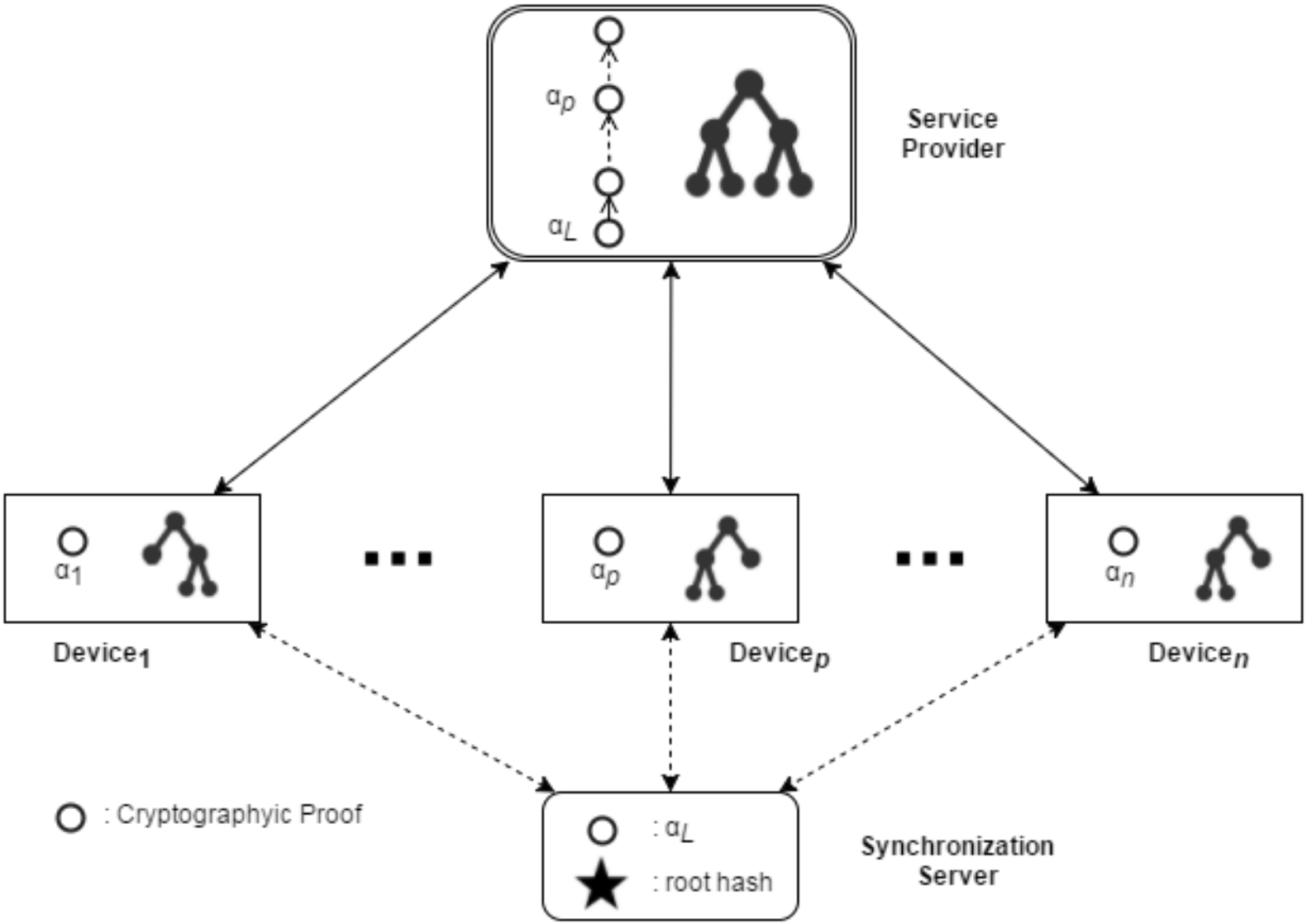


Merkle Tree


: 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)

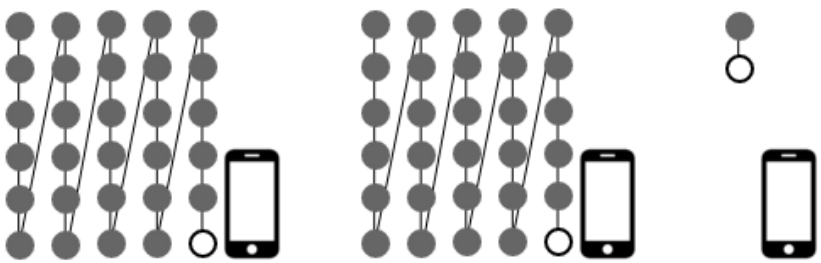
Real-time Proof of Violation for Cloud Storage

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



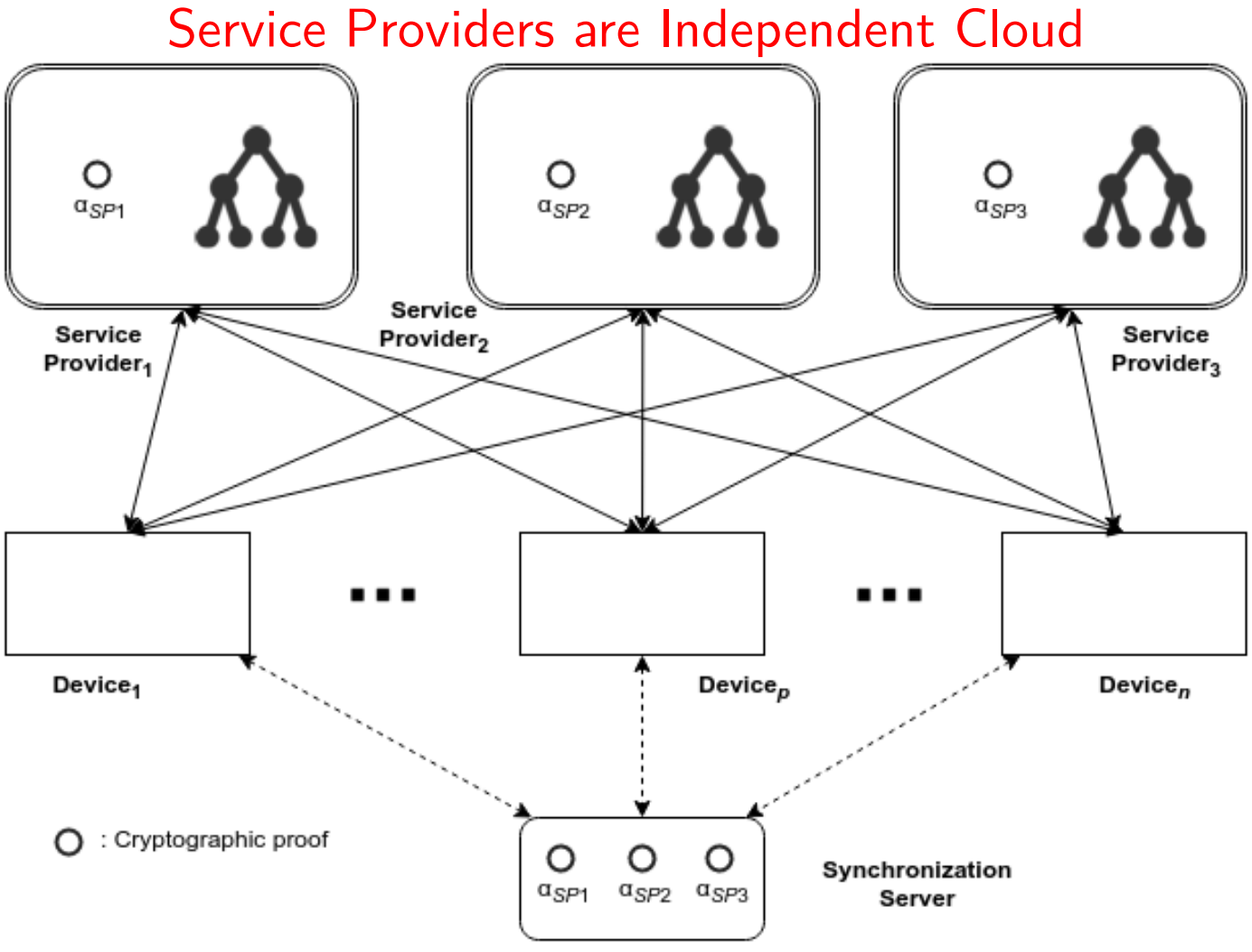
Worst-case

若有個 device 很久沒有使用
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: 同時有 k 個 server 回傳錯誤結果的機率 ≈ 0

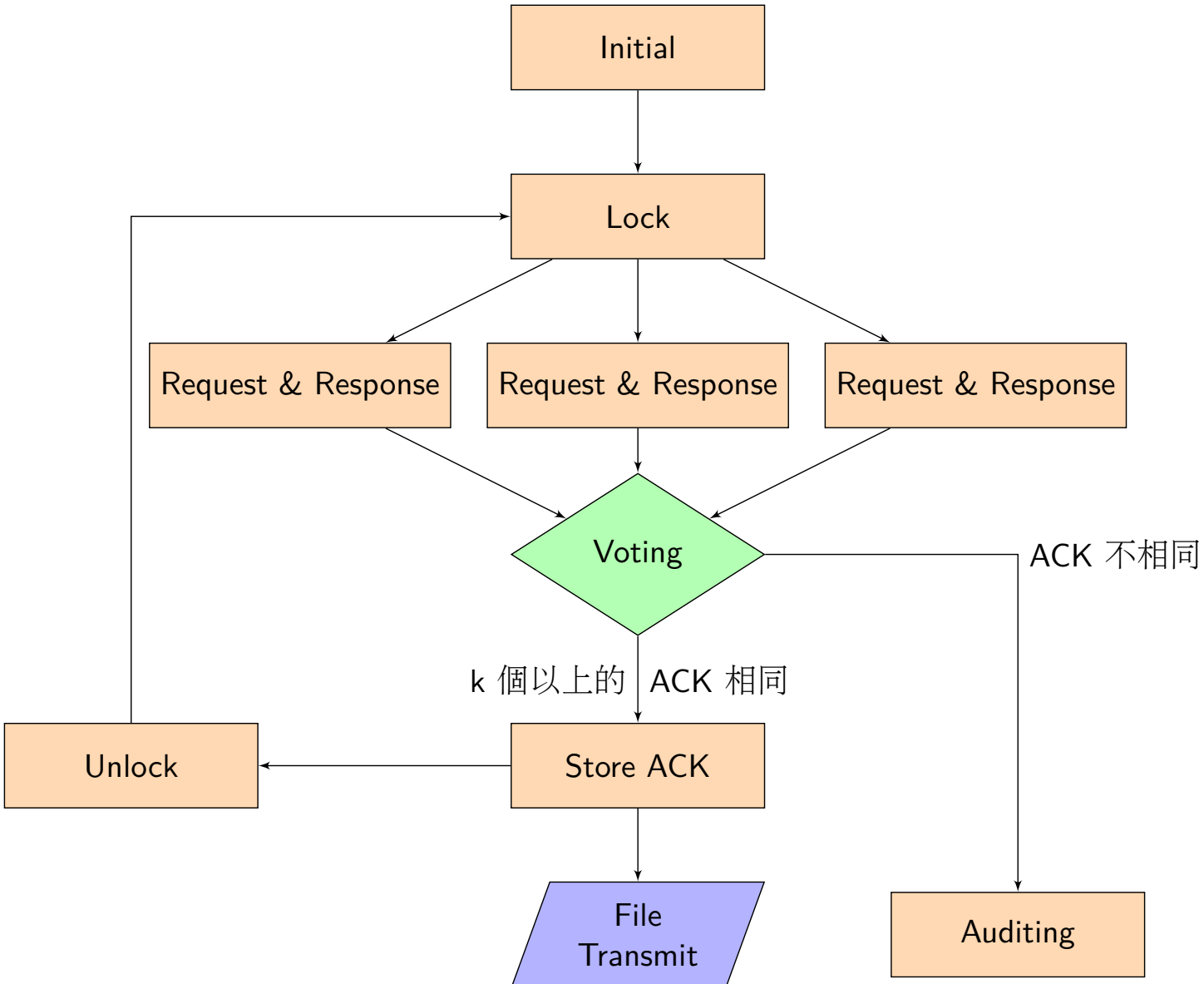


Comparison

- 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

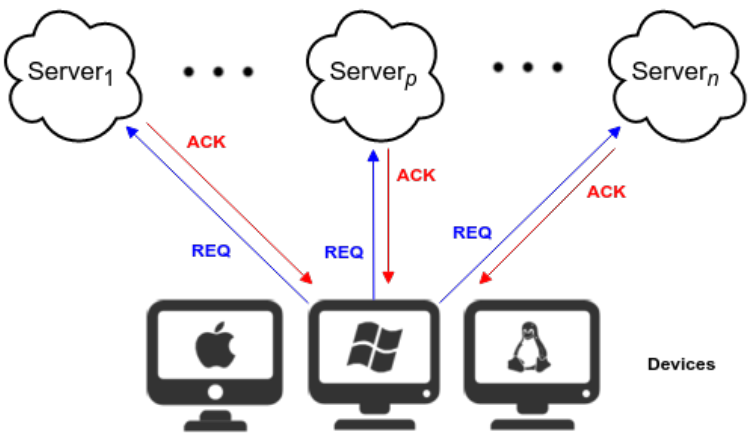
- Cons
  1. 需要傳送多份 Request, 處理多份 Response
  2. 需要使用較多的 Service Provider

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
File Transmit
Auditing

Download & Upload

Request & Response



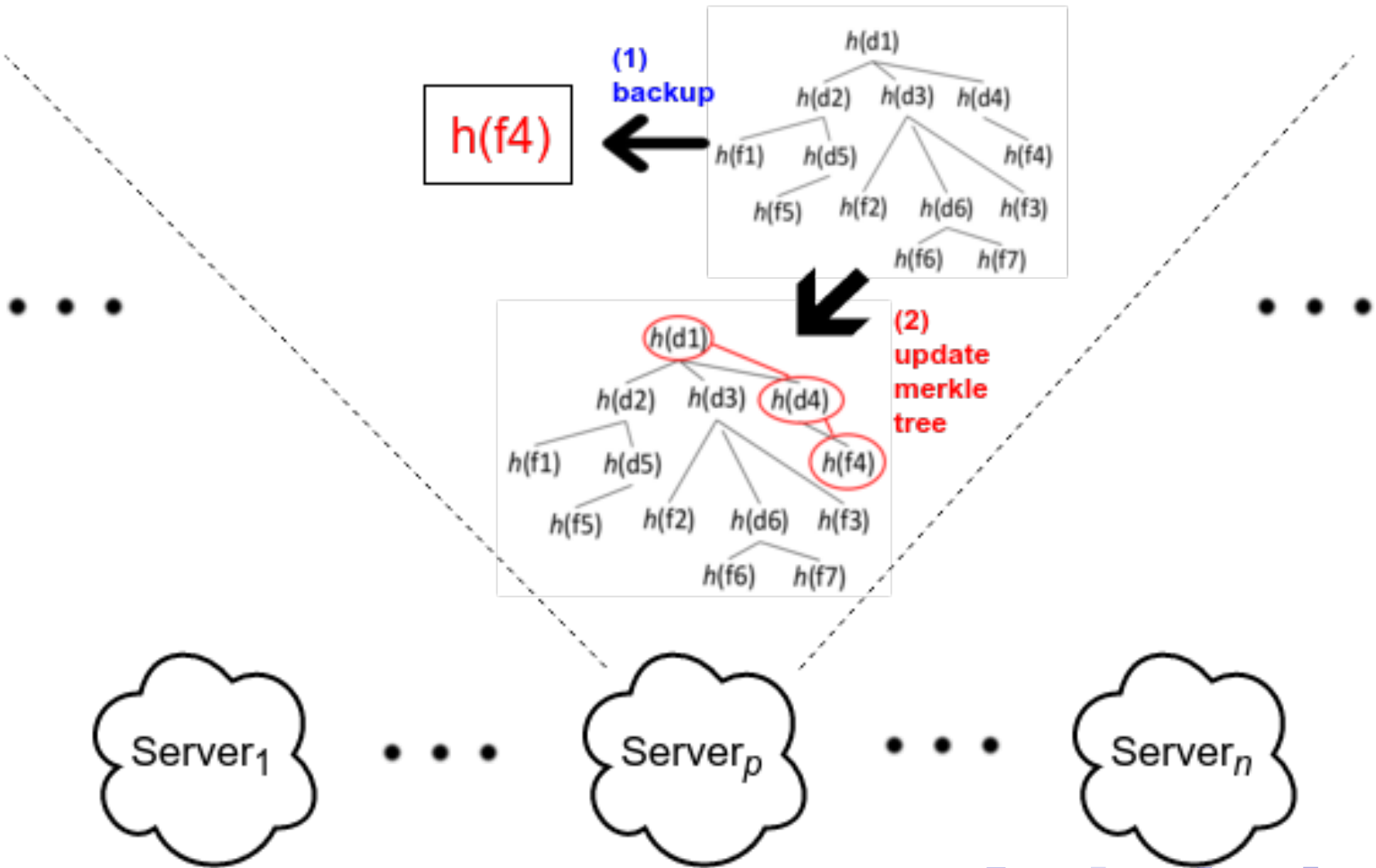
$$REQ = (OP,\ [OP]_{pri(D)})$$
$$OP = (TYPE,\ PATH,\ HASH,\ SN)$$
$$SN = \text{Sequence Number}$$

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

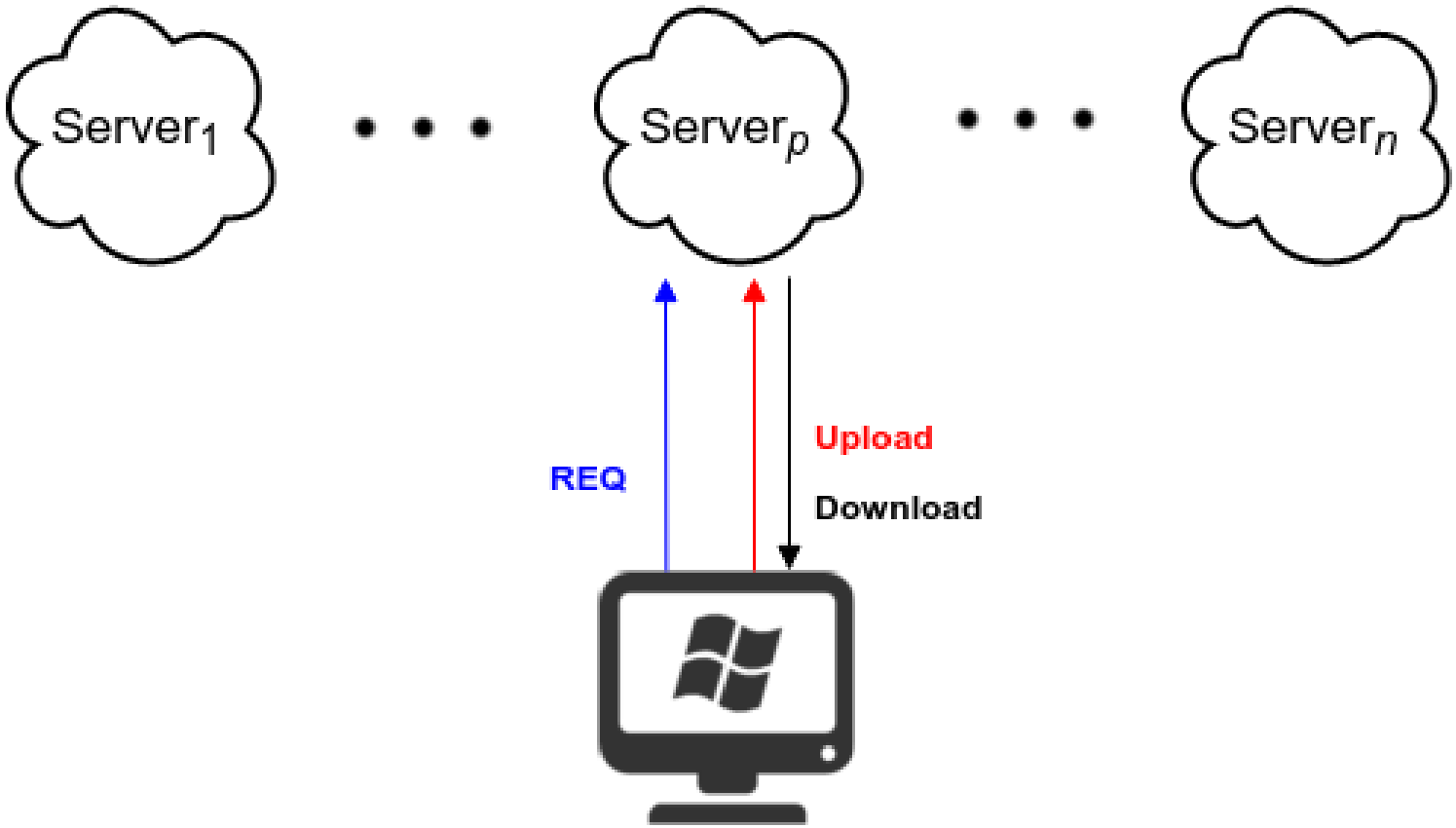
collect ACKs and voting

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

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	9.40653	0.00333	5.4 KB
B	55.14738	2.70313	5.08 MB
C	339.18192	0.3342	4.37 MB

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

	Serialize	Deserialize
A	0.04	0.009
B	0.756	0.299
C	0.67	0.295

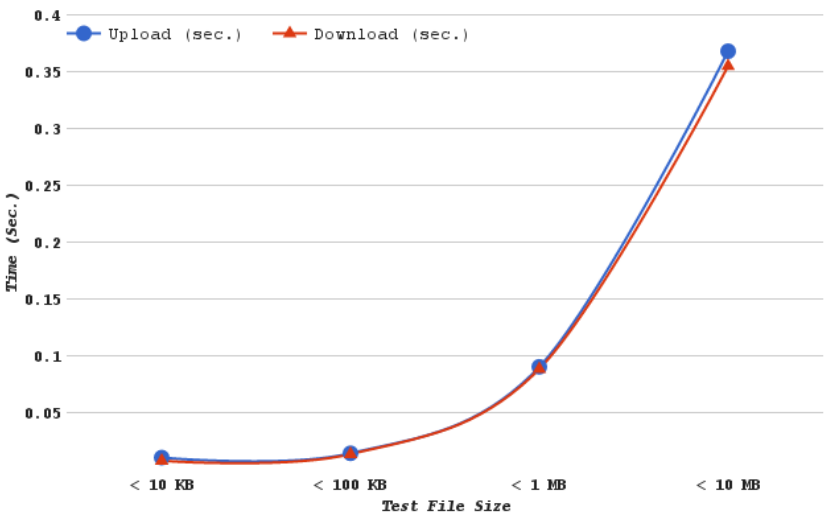
Experimental Results
Non POV

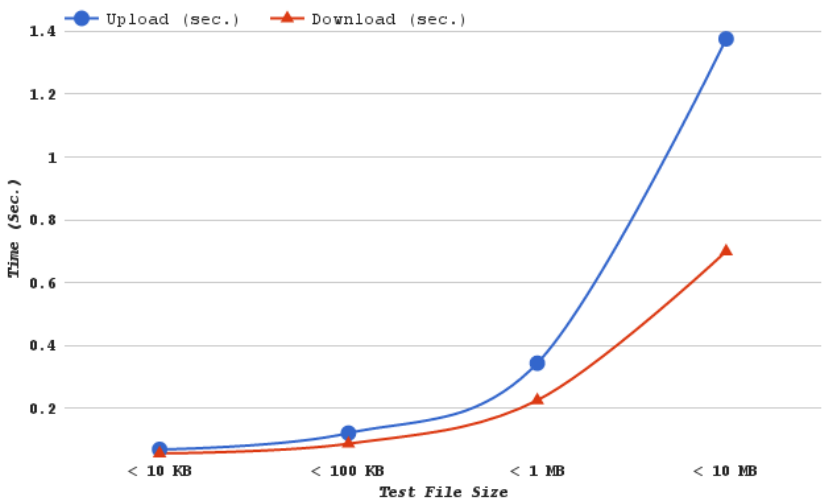
Table: The client device and SP are in the same network segment

	Upload (sec.)	Download (sec.)
<10 KB	0.010608	0.007845
<100 KB	0.014393	0.013691
<1 MB	0.090440	0.088570
<10 MB	0.367989	0.354916

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

	Upload (sec.)	Download (sec.)
<10 KB	0.069273	0.056629
<100 KB	0.121093	0.087351
<1 MB	0.343584	0.225566
<10 MB	1.675616	0.699524



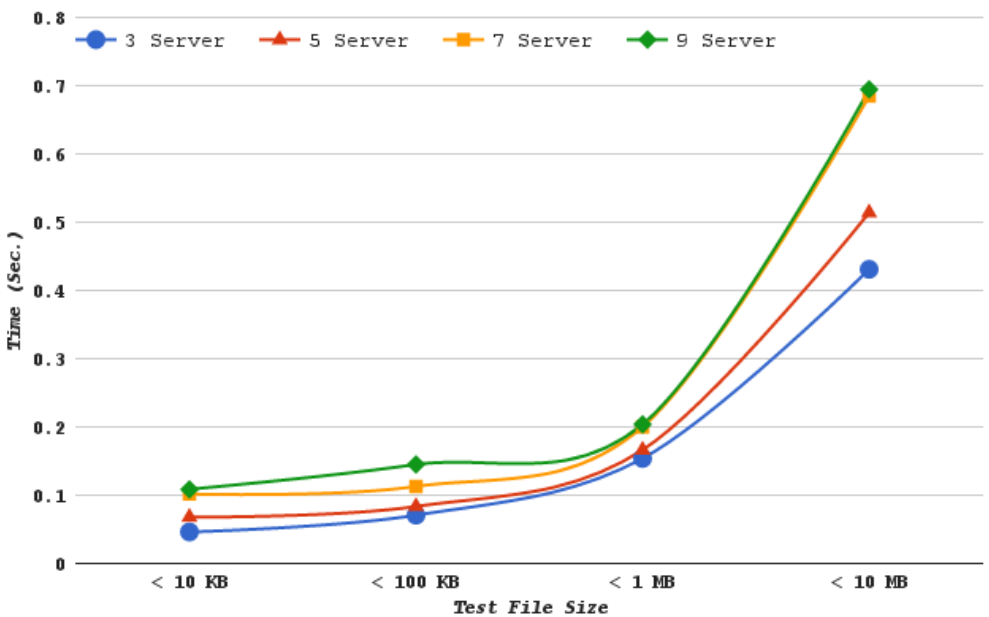


Experimental Results

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	0.046139	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

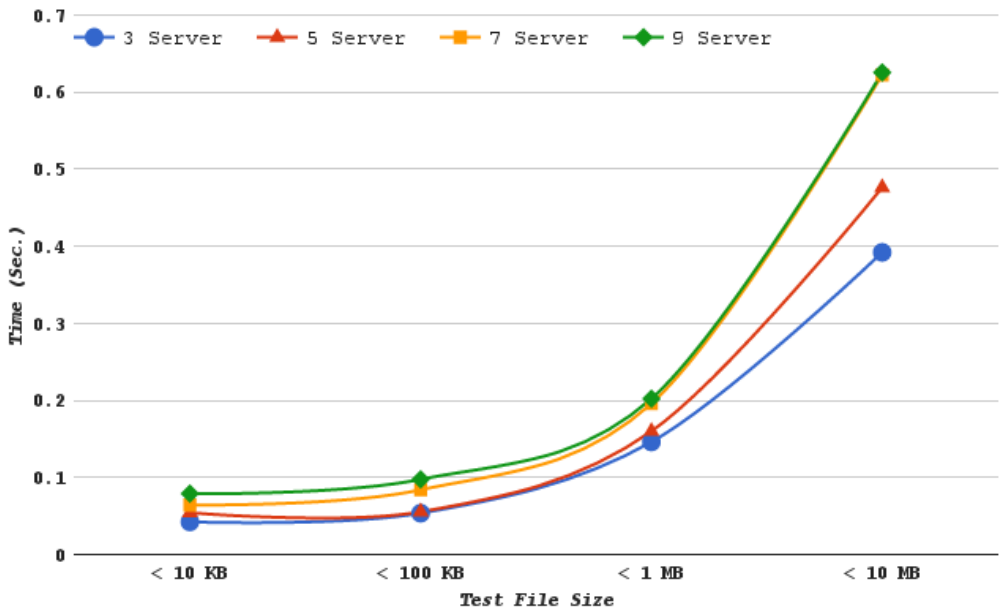


Experimental Results

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	0.042295	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

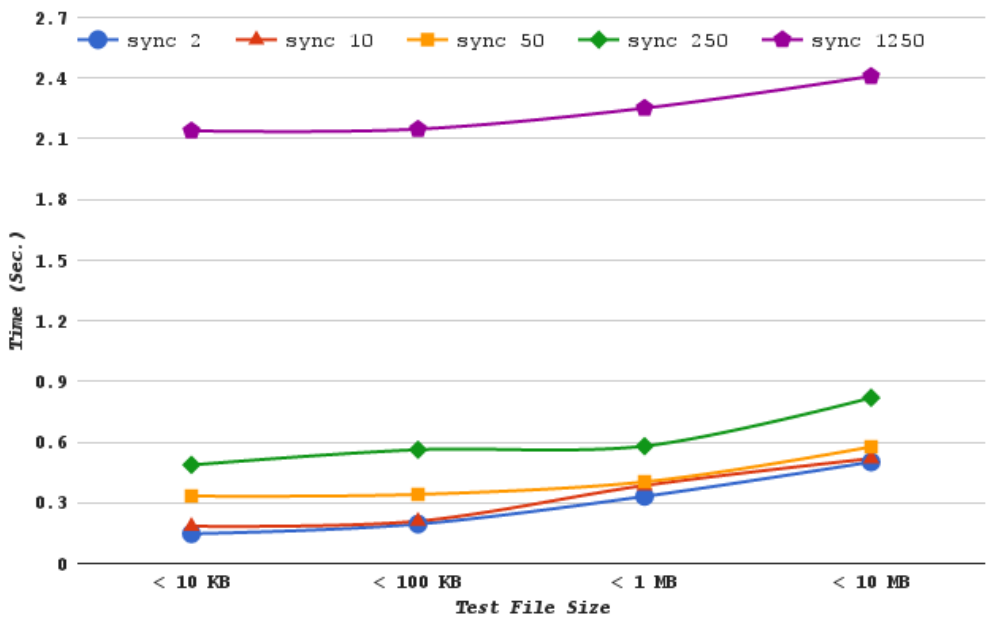


Experimental Results

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	0.146783	0.184138	0.332988	0.486858	2.139086
<100 KB	0.194642	0.209044	0.341408	0.562457	2.147664
<1 MB	0.331595	0.385494	0.403481	0.580193	2.251284
<10 MB	0.501692	0.518835	0.576403	0.819175	2.409135

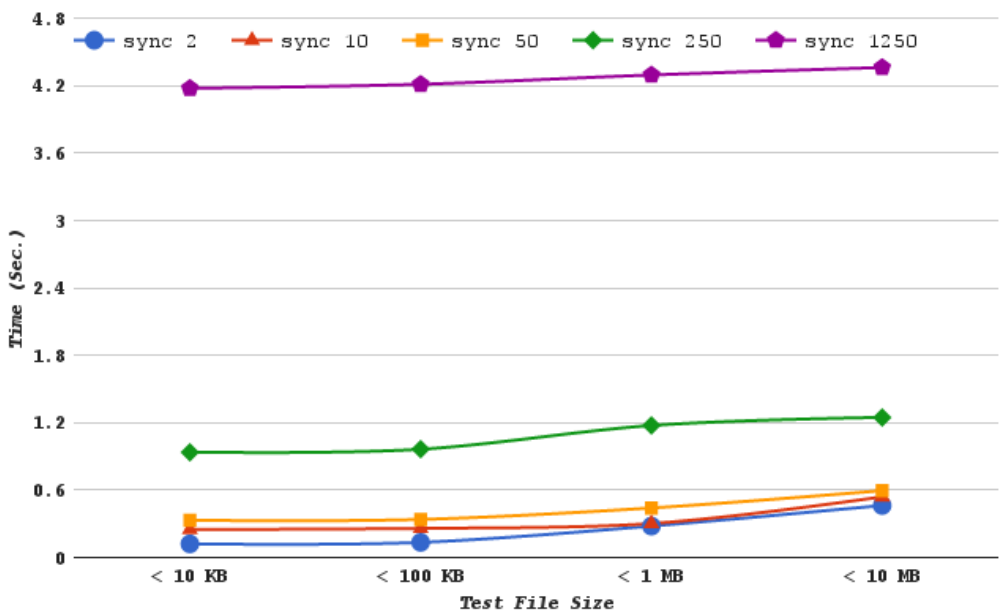


Experimental Results

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

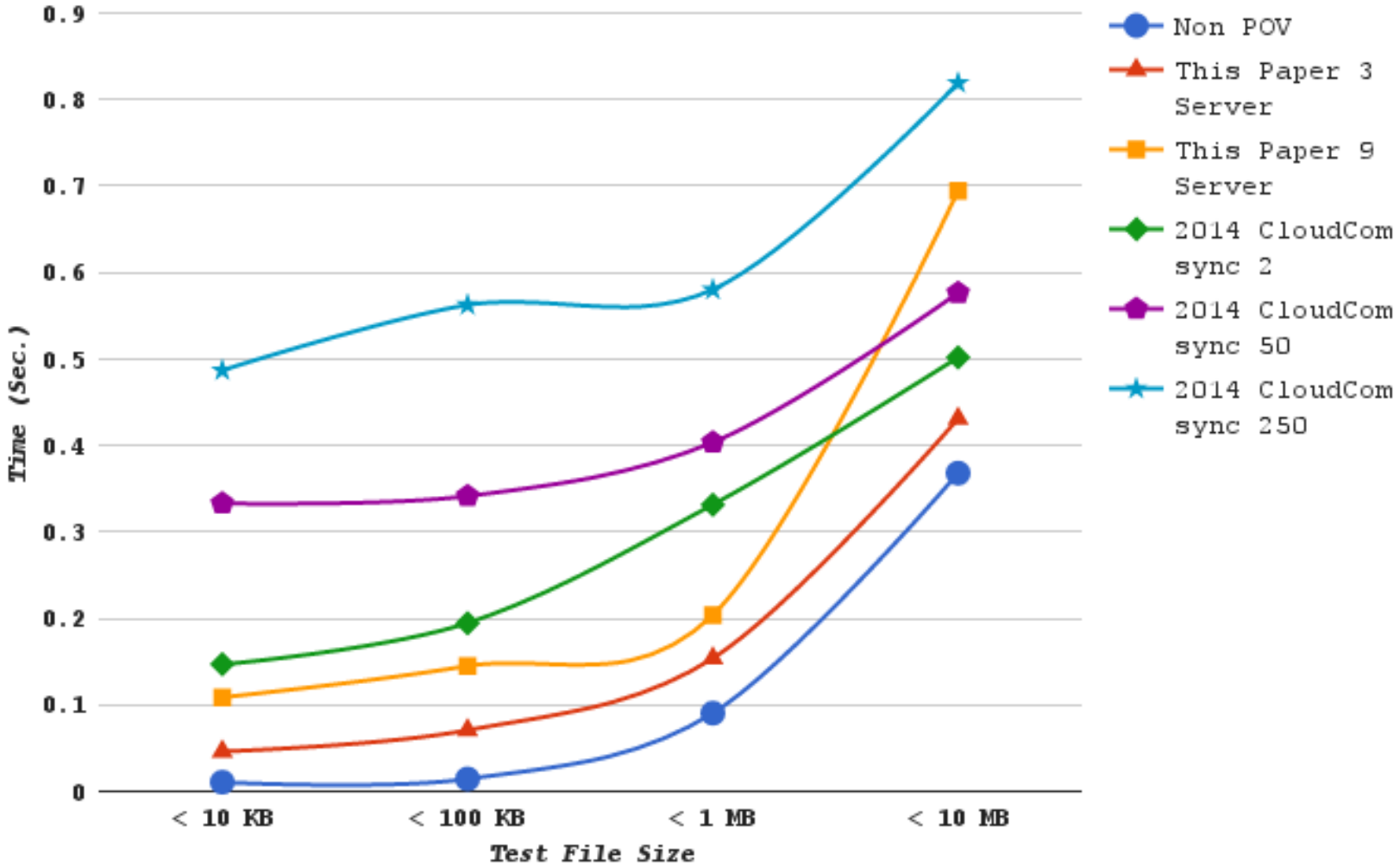
Table: THE EXECUTION TIME OF DOWNLOAD OPERATIONS (IN SEC.) (Account C)

	sync 2	sync 10	sync 50	sync 100	sync 500
<10 KB	0.121268	0.249803	0.331339	0.937337	4.175263
<100 KB	0.134563	0.258717	0.338794	0.963107	4.211038
<1 MB	0.279563	0.302230	0.440841	1.174882	4.294038
<10 MB	0.462677	0.539638	0.595140	1.247275	4.360539



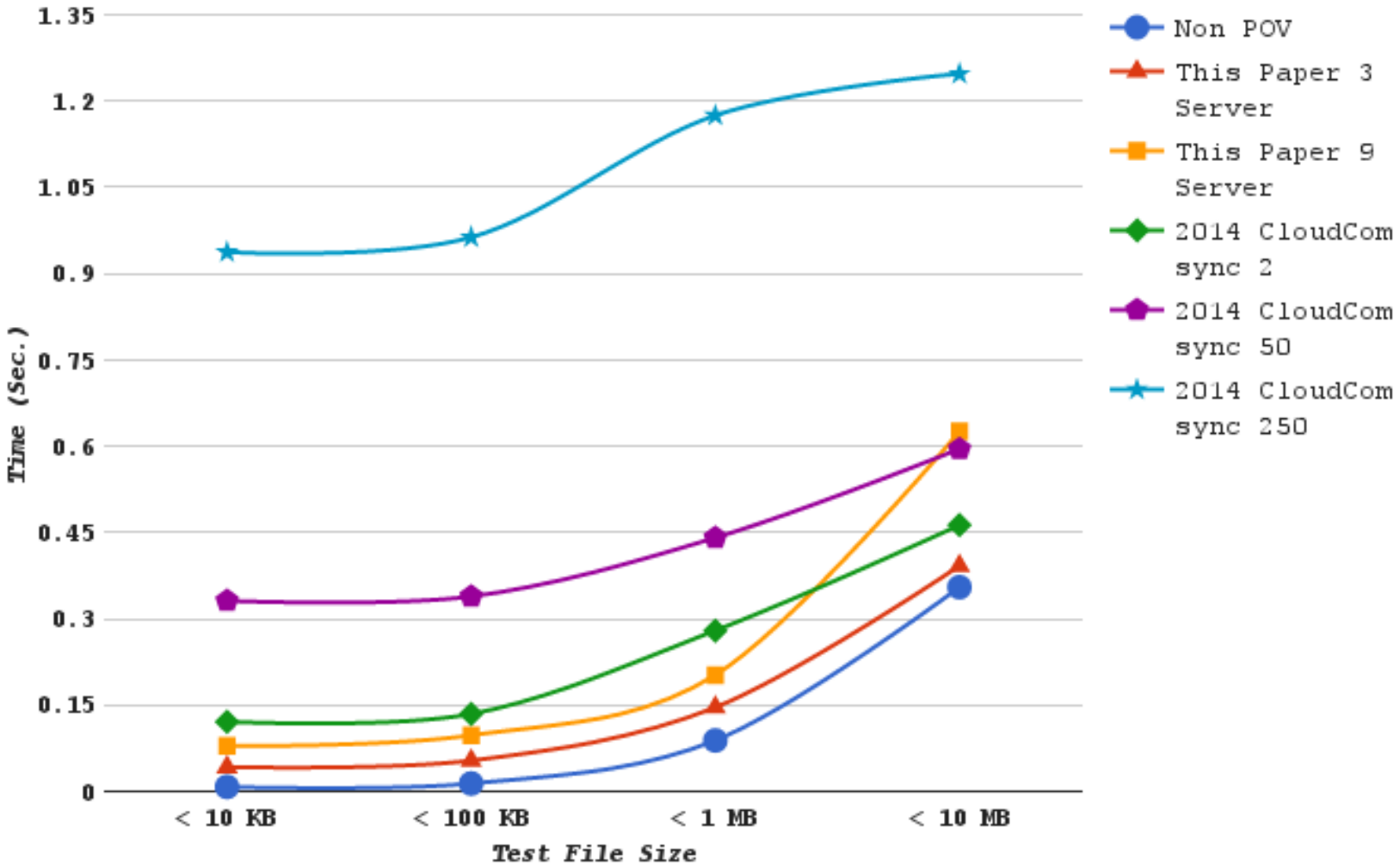
Experimental Results

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	4.349552	6.403042	9.584967	10.246768
<100 KB	4.914887	5.805870	7.843824	10.077857
<1 MB	1.700816	1.838656	2.211983	2.254196
<10 MB	1.171060	1.396453	1.860562	1.886630

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

	sync 2	sync 10	sync 50	sync 250	sync 1250
<10 KB	13.837201	17.358624	31.390677	45.895962	201.651193
<100 KB	13.523544	14.524231	23.720780	39.079062	149.217959
<1 MB	3.666447	4.262410	4.461293	6.415199	24.892477
<10 MB	1.363336	1.409920	1.566359	2.226087	6.546762

Avg: 6.61 times, Max: 19.67 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	5.391663	6.917309	8.205786	10.054378
<100 KB	3.913722	4.049482	6.132484	7.121880
<1 MB	1.648657	1.805003	2.210875	2.283095
<10 MB	1.104689	1.341869	1.754401	1.762387

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

	sync 2	sync 10	sync 50	sync 250	sync 1250
<10 KB	15.459033	31.844389	42.238325	119.489570	532.253193
<100 KB	9.828453	18.896670	24.745459	70.345135	307.573438
<1 MB	3.156419	3.412343	4.977329	13.265056	48.482022
<10 MB	1.303623	1.520467	1.676847	3.514280	12.286111

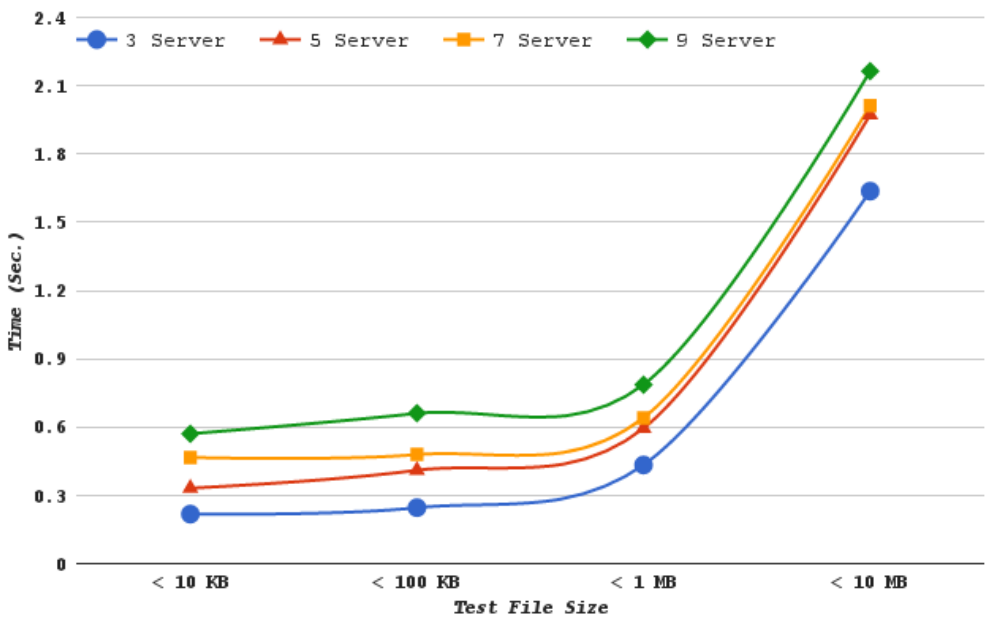
Avg: 15.41 times, Max: 52.93 times

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	0.217563	0.331341	0.466655	0.570460
<100 KB	0.245769	0.410174	0.479227	0.660178
<1 MB	0.433338	0.594532	0.640597	0.786688
<10 MB	1.636473	1.972134	2.011500	2.163858

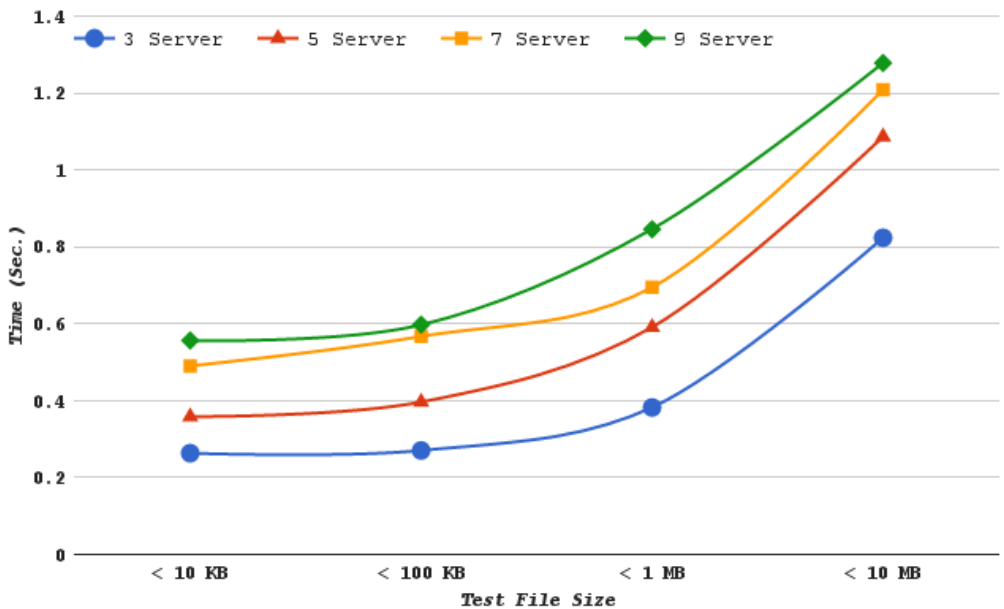


Experimental Results

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	0.263332	0.358435	0.490343	0.556110
<100 KB	0.270404	0.396497	0.567059	0.597088
<1 MB	0.382264	0.590987	0.694622	0.846141
<10 MB	0.823476	1.086515	1.208293	1.278169

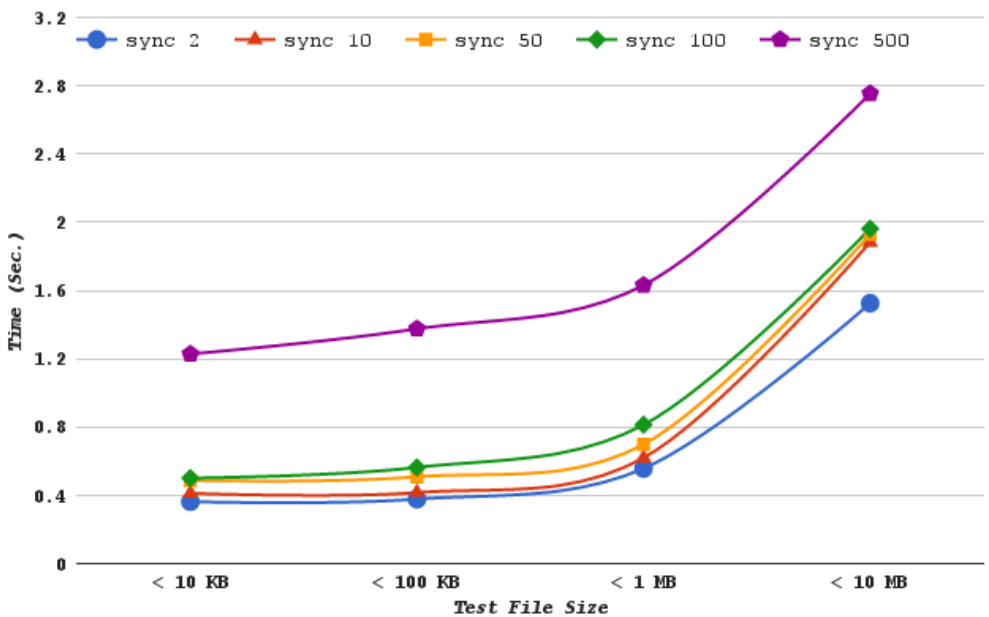


Experimental Results

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	0.362766	0.411929	0.486570	0.500776	1.227709
<100 KB	0.377788	0.416367	0.508769	0.563544	1.375298
<1 MB	0.556890	0.619318	0.698361	0.812837	1.630702
<10 MB	1.525459	1.882746	1.929606	1.962343	2.753549

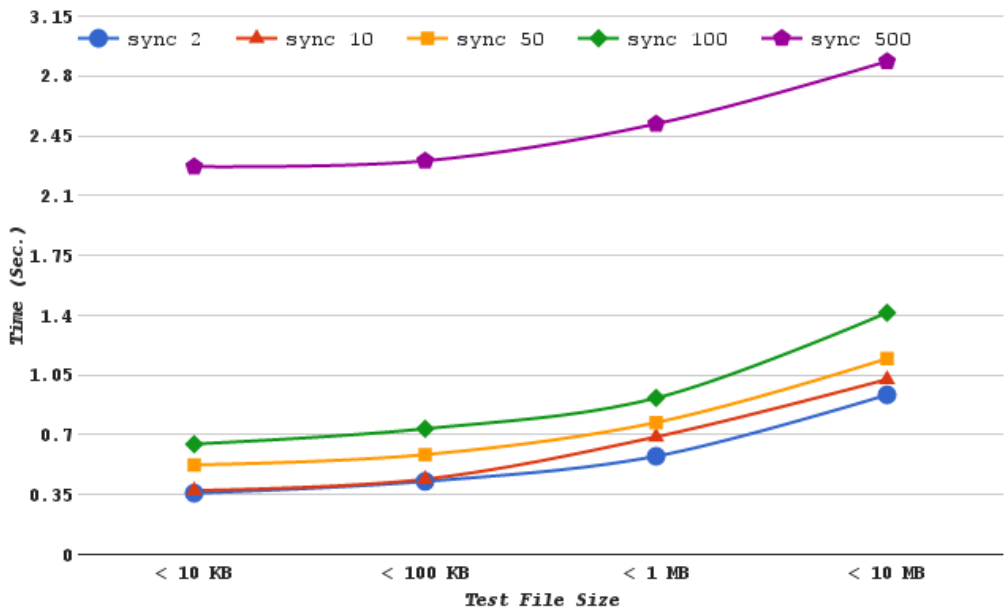


Experimental Results

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

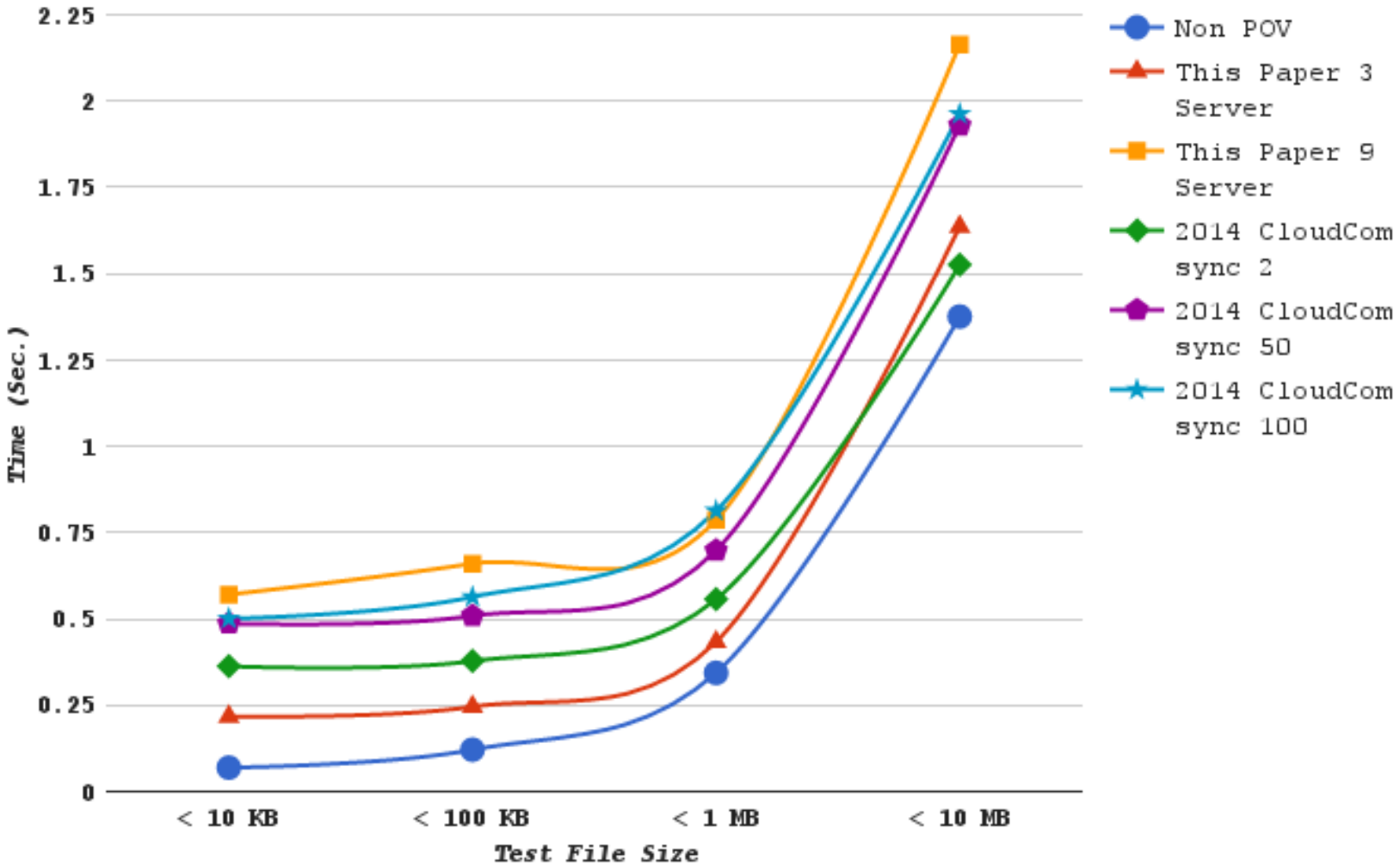
Table: THE EXECUTION TIME OF DOWNLOAD OPERATIONS (IN SEC.) (Account C)

	sync 2	sync 10	sync 50	sync 100	sync 500
<10 KB	0.388520	0.374224	0.524074	0.646150	2.269309
<100 KB	0.427226	0.440348	0.584122	0.735439	2.302957
<1 MB	0.574539	0.687956	0.772134	0.914938	2.519163
<10 MB	0.933868	1.024385	1.145598	1.414567	2.884841



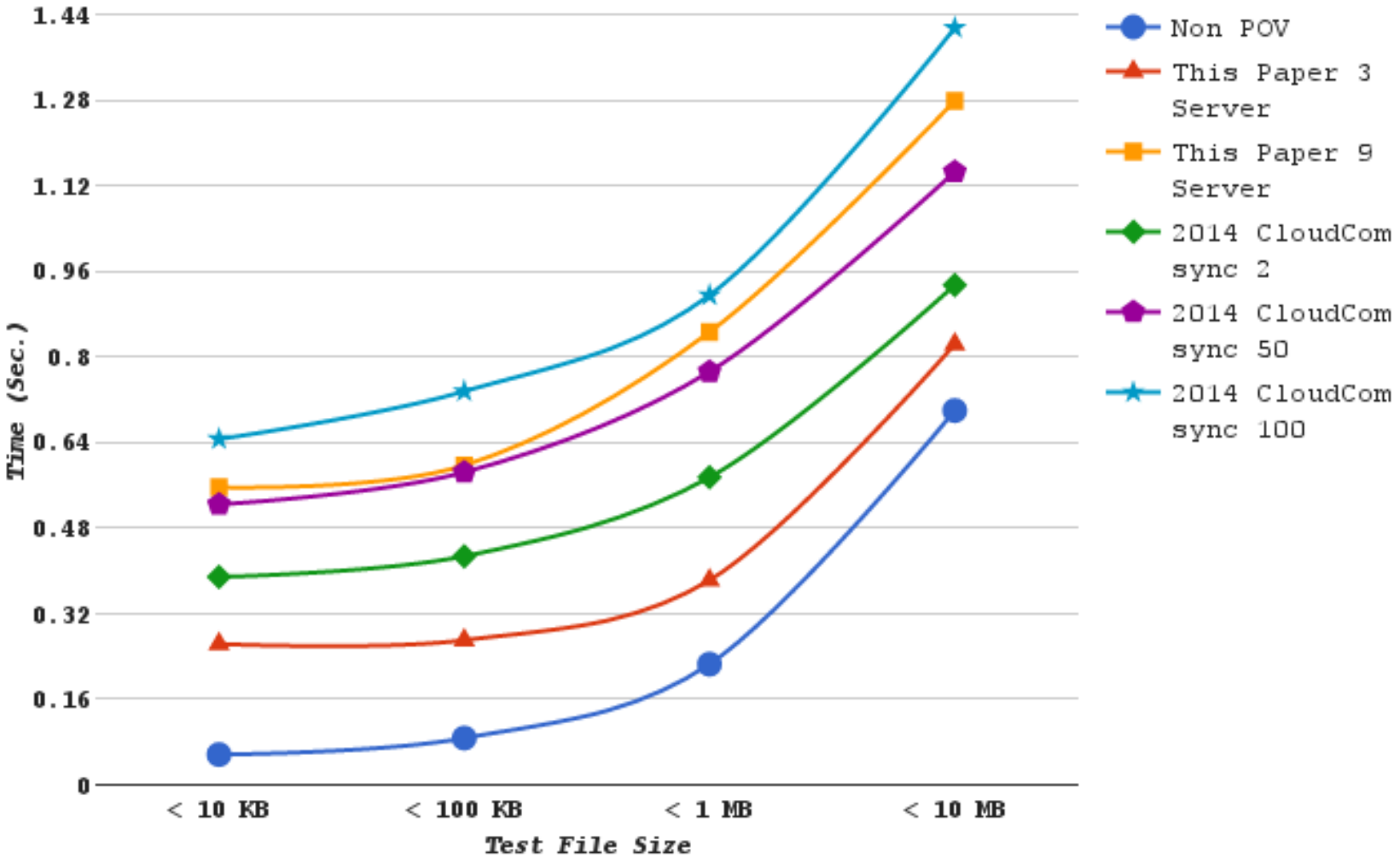
Experimental Results

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	3.140669	4.783127	6.736478	8.234973
<100 KB	2.029588	3.387261	3.957507	5.451819
<1 MB	1.261228	1.730382	1.864455	2.289650
<10 MB	1.189629	1.433637	1.462254	1.573011

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

	sync 2	sync 10	sync 50	sync 100	sync 500
<10 KB	5.236767	5.946479	7.023971	7.2290	17.7228
<100 KB	3.119815	3.438406	4.201470	4.6538	11.3574
<1 MB	1.620825	1.802520	2.032574	2.3658	4.7461
<10 MB	1.108928	1.368657	1.402722	1.4265	2.0017

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	4.650108	6.329503	8.658827	9.820191
<100 KB	3.095611	4.539142	6.491742	6.835527
<1 MB	1.694689	2.620022	3.079470	3.751199
<10 MB	1.177195	1.553220	1.727308	1.827199

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

	sync 2	sync 10	sync 50	sync 100	sync 500
<10 KB	6.860769	6.608313	9.254478	11.4102	40.0731
<100 KB	4.890921	5.041151	6.687090	8.4194	26.3645
<1 MB	2.547104	3.049914	3.423100	4.0562	11.1682
<10 MB	1.335005	1.464403	1.637682	2.0222	4.1240

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 6 倍以上的時間，
Worst-case 時更能夠節省超過 50 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 (SLA) 中

Future Work

1. 我們希望能將 FBH 樹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，
將將能讓我們的架構更加的彈性且使用更少的硬體。

Thanks for Your Listening