科技部資訊安全技術研發專案計畫

『系統測試報告書』

System Testing Document

建立雲端系統交互信任的行為違反證明技術之進階研究

Advanced Study on Schemes of Proof of Violation for Mutual Trust in Cloud Systems

MOST 104-2221-E003-014 -

黃冠寰教授

雲端運算實驗室

國立台灣師範大學資訊工程學系

目錄

版本變更紀錄 (Revision History)

版次	變更項目	變更日期
1.0	第一版	2016.06.07
2.0	增加測試環境、效能比較與測試結果分析	2016.07.10

第一章 介紹

雲端系統已成為資訊系統中發展的主流，也成為人們生活的一部份。目前雲端系統的發展中，建立交互不可否定性（Mutual non-repudiation）及信任（Trust）是最重要的課題之一。很多機構、政府、公司甚或個人因為對於雲端系統所提供服務的安全性尚有疑慮，因此還不敢使用雲端服務。若我們能成功的於雲端系統發展交互不可否定性及信任，將可進一步推進雲端系統的普遍性。

本計劃目標為研發行為違反證明（Proof of Violation, POV）技術。POV 技術使得使用者於取得雲端服務時能留下證據（Attestation）並於有爭議時用於證明（Proof）雲端系統有或沒有違反合約中所約定的特性（Properties）。

雲端系統發展的一大阻礙是可能的使用者對雲端服務沒有信任感。POV 技術能在使用者和服務提供者間建議交互信任。然而現今對於 POV 技術的研究僅限於雲端儲存系統，我們在本年度中研究如何在雲端 SOA 系統上建立 POV 機制，提出了四種多向交握的協定（Multistep handshake protocol）：

- Two-Step-SN
- Two-Step-CH
- Four-Step-C&L
- Four-Step-DH

我們將這四種協定整合在同一個系統中，使用者在與系統發送請求時，能夠指定以何種協定進行訊息交換，每種協定都提供上傳資料、下載資料以及稽核證據等三種功能，其中，Four-Step-C&L 與 Four-Step-DH 支援多個使用者同時請求同一個資料實體。而在所有使用者和系統溝通的訊息中都帶有電子簽章，我們在稽核時不僅會檢查所有證據的順序性，還會驗證證據上面的電子簽章是否有效。

第二章 系統測試說明

第一節 目的

本測試目的在於測試四種 POV 協定的功能，測試是否有達到我們在發展這四個協定時所預期的功能以及他們的效能比較，並將所得到的測試記錄製作成報告書，交由科技部審查我們的研究成果可用性。

第二節 測試重點

1. 四種 POV 協定的功能：檔案上傳、檔案下載與稽核證據。
2. 每個驗證測試案例執行後，確定功能或執行特性是否滿足預期的需求。
3. 測試過程中記錄每種 POV 協定所花費的時間，製成校能比較表。
4. 僅使用黑箱測試

第三節 測試環境

	服務提供者	使用者
地理位置	日本東京 (Amazon EC2)	台灣台北
作業系統	Ubuntu 14.04.3 LTS	CentOS 6.6
CPU 規格	Intel® Xeon® CPU E5-2676 v3	Intel® Xeon® CPU E5-2643
主記憶體大小	1 GiB	8 GiB

我們使用 iperf3 測量兩者之間的傳輸頻寬，結果為 55.8 Mbits/sec。

第四節 測試流程

啟動系統之後，使用者輪流挑選四種 POV 協定做測試。首先，交叉進行檔案上傳與下載的動作，我們提供三種不同大小的檔案供使用者選擇：1MB、10MB、100MB，對每種協定分別交叉做檔案上傳十次、下載十次，也就是最後每種協定會留下二十筆證據，並紀錄所花費的時間。接下來是做稽核的動作，檢查上面的電子簽章與這二十次交叉上傳下載的順序是否正確，並記錄所花費的時間。

對於可以同步執行的 Four-Step-C&L 與 Four-Step-DH，我們用四名使用者同時執行上傳與下載動作，以測試其正確性。

第三章 系統功能測試

1. Two-Step-SN

表單代號：POV-01		功能測試		版本：V1.0
協定代號 / 名稱		功能代號 / 名稱		測試日期
Two-Step-SN		Two-Step-SN		105/6/6
測試項目				
項目	功能名稱	測試結果	測試結果描述	
1	上傳檔案	■ 通過 □ 未通過	上傳成功	
2	下載檔案	■ 通過 □ 未通過	下載成功	
3	稽核證據	■ 通過 □ 未通過	所有證據內的 sequence number 皆正確	

2. Two-Step-CH

表單代號：POV-02		功能測試		版本：V1.0
協定代號 / 名稱		功能代號 / 名稱		測試日期
Two-Step-CH		Two-Step-CH		105/6/6
測試項目				
項目	功能名稱	測試結果	測試結果描述	
1	上傳檔案	■ 通過 □ 未通過	上傳成功	
2	下載檔案	■ 通過 □ 未通過	下載成功	
3	稽核證據	■ 通過 □ 未通過	所有證據的 hash 值皆正確放置於下一筆證據內	

3. Four-Step-C&L

表單代號：POV-03		功能測試		版本：V1.0
協定代號 / 名稱		功能代號 / 名稱		測試日期
Four-Step-C&L		Four-Step-C&L		105/6/6
測試項目				
項目	功能名稱	測試結果	測試結果描述	
1	上傳檔案	■ 通過 □ 未通過	上傳成功	
2	下載檔案	■ 通過 □ 未通過	下載成功	
3	稽核證據	■ 通過 □ 未通過	所有使用者的 LSN 都各自正確連接，串連 response message 的 hashing chain 也正確	
4	同步執行下載檔案	■ 通過 □ 未通過	成功以四名使用者同時下載檔案	
5	同步執行上傳檔案	■ 通過 □ 未通過	由於 C&L 無法支援同步上傳不同檔案，但仍然正確讓使用者接連上傳	

4. Four-Step-DH

表單代號：POV-04		功能測試		版本：V1.0
協定代號 / 名稱		功能代號 / 名稱		測試日期
Two-Step-SN		Two-Step-SN		105/6/6
測試項目				
項目	功能名稱	測試結果	測試結果描述	
1	上傳檔案	■ 通過 □ 未通過	上傳成功	
2	下載檔案	■ 通過 □ 未通過	下載成功	
3	稽核證據	■ 通過 □ 未通過	所有使用者各自的 hashing chain 與大家共有的 hashing chain 皆正確	
4	同步執行下載檔案	■ 通過 □ 未通過	成功以四名使用者同時下載檔案	
5	同步執行上傳檔案	■ 通過 □ 未通過	成功以四名使用者同時上傳不同檔案	

第四章 校能比較

表一 四種 POV 協定校能比較表 (單位：毫秒)

	Two-Step-SN	Two-Step-CH	Four-Step-C&L	Four-Step-DH
1 MB	1329	1355	1110	908
10 MB	7472	7526	4295	4123
100 MB	68421	68916	38337	37724

表一中可以看出兩步驟 POV 協定的效能都比四步驟 POV 協定差，其原因不外乎是兩步驟的 POV 協定無法讓使用者同步執行上傳與下載檔案，而且這個校能上的差距在處理越大的檔案時越明顯。

表二 四種 POV 協定呼叫長時間服務的效能比較表 (單位：毫秒)

	Two-Step-SN	Two-Step-CH	Four-Step-C&L	Four-Step-DH
10 ms	1583	1613	1142	811
50 ms	5607	5626	5113	1581
100 ms	10615	10649	10116	2831
300 ms	30616	30646	30113	7819
500 ms	50622	50665	50118	12816
1000 ms	100628	100667	100121	25300

表二呈現了四種 POV 協定在呼叫長時間服務的效能比較，左邊欄位的 10 毫秒至 1000 毫秒代表所呼叫服務的平均處理時間。由於在這四種 POV 協定中，只有 Four-Step-DH 可以平行處理請求，可以看出在表三的結果中，Four-Step-DH 的效能相當突出，它可以同時處理四位使用者的請求，因此在處理長時間服務的效能上是其他三種 POV 協定的四倍。

表三 四種 POV 協定稽核 N 筆證據效能比較表 (單位：毫秒)

N / Protocol	10	100	1000	10000
Two-Step-SN	33	119	598	5777
Two-Step-CH	36	126	676	6627
Four-Step-C&L	40	181	1434	14011
Four-Step-DH	44	198	1531	14716

我們將四種 POV 協定稽核不同數量的證據所花費的時間記錄在表三之中，在稽核的過程中，每一筆證據的電子簽章都必須被驗證，以及根據不同的 POV 協定有不同的項目需要檢查，例如 Two-Step-SN 的序號（sequence number）、Two-Step-CH 的雜湊值、Four-Step-C&L 的序號及雜湊值和 Four-Step-DH 的兩個雜湊值。

在表三的結果可以看到四步驟 POV 協定的稽核所需時間大約是兩步驟的 POV 協定的一倍，因為四步驟 POV 協定的證據中包含的電子簽章數量是兩步驟 POV 協定證據的一倍，我們合理推論這裡的效能差距來自於驗證電子簽章所花費的時間。

第五章 測試結果分析

我們可以從第三章看出四種 POV 協定的功能已被正確實做，而效能的比較則完整的呈現在第四章。本章要再針對四種POV 協定的功能做一個完善的比較，如表四中所示。

表四 四種 POV 協定比較表

	Two-Step-SN	Two-Step-CH	Four-Step-C&L	Four-Step-DH
證據不可否認性	是	是	是	是
使用者須保持所有證據	是	否	否	否
多個使用者不須互相溝通即可輪流請求服務	否	否	是	是
在四步驟 POV 協定中，執行結果必須在第二步驟時準備好			是	否
可避免網路壅塞	否	否	否	是

首先，我們提出的四種 POV 協定所交換的訊息都包含訊息傳送者的電子簽章，因此皆有達成不可否認性。第二，只有在 Two-Step-SN 中需要保存所有的證據以便稽核，他需要比對每筆證據中的序號，而其他三種 POV 協定都只要存一個雜湊值就可以代表整條雜湊鏈的狀態，因此不需要存全部的證據。第三，當多位使用者想對同一個資料個體做存取時，使用 Two-Step-SN 與 Two-Step-CH 都比需互相交換最新一筆證據的序號或是雜湊值，而對 Four-Step-C&L 而言，每位使用者有自己的序號，Four-Step-DH 的每位使用者擁有自己的一條雜湊鏈，因此只有兩步驟的 POV 協定需要每位使用者互相交換資料。第四，使用 Four-Step-C&L 時，如果沒有把執行結果在第二步驟時準備好，服務提供者將會有假造執行結果的機會，而 Four-Step-DH 則可以避免此問題發生。第五，只有 Four-Step-DH 有機會在壅塞的網路中運行。

讓使用者信任雲端環境是一個非常重要的課題,我們提出了四種POV協定,其中以 Four-Step-DH 的分析結果最為亮眼，它能夠滿足各項分析條件。雲端服務提供者可以使用 Four-Step-DH 來讓使用者請求服務，不但能讓雙方都留下互相不可否認的證據，還可以保持服務的效能及品質。