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

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，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. 僅使用黑箱測試

第三節 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。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。

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	