行政院國家科學委員會專題研究計畫 成果報告

前瞻性雲端安全儲存、防護、行為分析與觀測平台--子計畫一：支援多樣功能之雲端資料安全儲存(2/2)
研究成果報告(完整版)

計 畫 類 別 ：整合型
計 畫 編 號 ：NSC 100-2218-E-009-006-
執 行 期 間 ：100 年 08 月 01 日至 101 年 07 月 31 日
執 行 單 位 ：國立交通大學資訊工程學系（所）

計 畫 主 持 人：曾文貴

計畫參與人員：碩士班研究生-兼任助理人員：陳彥宇
碩士班研究生-兼任助理人員：戴靜瑤
碩士班研究生-兼任助理人員：謝維揚
博士班研究生-兼任助理人員：沈宣佐

公 開 資 訊 ：本計畫可公開查詢

中 華 民 國 101 年 11 月 01 日

中 文 摘 要 ： 本研究計畫研究主題為支援多樣功能之雲端資料安全儲存。安全性要求是雲端系統必備的條件之一，我們所關注的問題主要為儲存安全與計算安全。除了保障使用者儲存的資料不會在未經許可下被窺視和竄改外，系統也需保障使用者儲存的資料不會因為儲存裝置的毀損而遺失。而在此同時，若系統能提供多樣性的功能，如錯誤修正、內容分享、存取控制等，將使得雲端基礎建設功能性更加完備。
我們研究的成果有 (1) 保護隱私的雲端偵測入侵系統；(2) 雲端資料的存取控制；(3) 非集中式雲端儲存系統中系統修復機制之研究；及 (4) 資料完整性授權驗證。

中文關鍵詞： 分散式雲端儲儲存與修復、金鑰存取控制、授權完整性檢查，雲端入侵偵測

英 文 摘 要 ： In this project, we study secure cloud storage supporting multi-functionality. One of the requisitions of a cloud system is security. We mainly focus on secure storage and secure computation. In addition to prevent the unauthorized access and modification of user data, the system has to guarantee that user data are not missed even if some of the storage server is damaged. Simultaneously, the cloud system can be more complete if it can support multiple functionalities, such as, error correcting, content sharing, and access control.
In this year, our research results consist of: (1) privacy preserving cloud intrusion detection system; (2) hierarchical key access control for cloud storage; (3) the repair mechanism of decentralized cloud storage system; and (4) delegable data possession validation.

英文關鍵詞： repair mechanism for distributed cloud storage, key-controlled cloud access, delegated integrity check, cloud-based intrusion detection system.

行政院國家科學委員會補助專題研究計畫

期末報告

子計畫一：支援多樣功能之雲端資料安全儲存

計畫類別：□個別型計畫　☑整合型計畫
計畫編號：NSC-100-2218-E-009-006
執行期間：　99 年 8 月 1 日至　101 年　7 月 31 日
第二年度：　100 年 8 月 1 日至　101 年　7 月 31 日
計畫主持人：曾文貴 教授
計畫參與人員：沈宣佐、陳彥宇、戴靜瑤、謝維揚

成果報告類型(依經費核定清單規定繳交)：□精簡報告　☑完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立交通大學 資訊工程學系

中　華　民　國 101 年 10 月 30 日

中文摘要

本研究計畫研究主題為支援多樣功能之雲端資料安全儲存。安全性要求是雲端系統必備的條件之一，我們所關注的問題主要為儲存安全與計算安全。除了保障使用者儲存的資料不會在未經許可下被窺視和竄改外，系統也需保障使用者儲存的資料不會因為儲存裝置的毀損而遺失。而在此同時，若系統能提供多樣性的功能，如錯誤修正、內容分享、存取控制等，將使得雲端基礎建設功能性更加完備。

我們研究的成果有 (1) 保護隱私的雲端偵測入侵系統；(2)雲端資料的存取控制；(3) 非集中式雲端儲存系統中系統修復機制之研究；及 (4) 資料完整性授權驗證。

關鍵詞: 分散式雲端儲儲存與修復、金鑰存取控制、授權完整性檢查，雲端入侵偵測

英文摘要:

In this project, we study secure cloud storage supporting multi-functionality. One of the requisitions of a cloud system is security. We mainly focus on secure storage and secure computation. In addition to prevent the unauthorized access and modification of user data, the system has to guarantee that user data are not missed even if some of the storage server is damaged. Simultaneously, the cloud system can be more complete if it can support multiple functionalities, such as, error correcting, content sharing, and access control.

In this year, our research results consist of: (1) privacy preserving cloud intrusion detection system; (2) hierarchical key access control for cloud storage; (3) the repair mechanism of decentralized cloud storage system; and (4) delegable data possession validation.

Keywords: repair mechanism for distributed cloud storage, key-controlled cloud access, delegated integrity check, cloud-based intrusion detection system.

1. 計畫緣起及目的

在技術發展史上來看，分散式系統已經有初期的雲端概念，然而當時並沒有普及的網路架構與隨身可上網的裝置作為基礎，現今完善的網路環境則啟動了雲端技術的蓬勃發展。整個雲端的架構可以說是將早期的大型主機與終端機架構中主機到終端機的連線改為網路媒介，另外將單一主機改為大型伺服器群組。雲端議題之所以倍受關注，它表彰的精減成本精神是最切合企業需要的部份，更呼應了當前全球節能減碳的大趨勢。

雲端帶來了許多好處，技術瓶頸慢慢被突破，雲端服務已經開始充斥在一般民眾的日常生活之中。但是當資料大量集中到雲端裡面的時候，就衍生了許多安全議題。有別於以往個人電腦的安全問題，在雲端裡面若發生安全性的問題，後果可能是影響到所有在雲端活動的使用者。因此，安全性要求是雲端系統必備的條件之一，而除了保障使用者儲存的資料不會在未經許可下被窺視和竄改外，若系統能提供多樣性的功能（如錯誤修正、內容分享、存取控制等）將使得雲端基礎建設功能性更加完備。

本計畫的研究主題為支援多樣功能之雲端資料安全儲存。針對雲端平台，我們所關注的問題可分為儲存安全與計算安全。針對這些問題，我們的研究如下：

(1) 儲存安全

在大型且分散式的環境中，任一個機器都有可能突然毀損，在這樣的先天條件中，要透過甚麼樣的儲存方式可以達到所有的資料都不會遺失，使得整體系統仍能正常提供服務。其中最直接的容錯技術就是儲存副本，例如磁碟陣列或早期許多分散式儲存系統。但是，副本技術提供的容錯能力付出了很大的儲存成本。為了解決這個問題，Erasure codes被提出可以應用到容錯儲存上，RAID-5與RAID-6就應用了Erasure codes的技術。雖然目前已有許多類似技術，但到目前為止尚未有一個方法可以低儲存成本達到快速且能夠容忍隨機且大量的儲存毀損。

此外，儲存資料隱私性也是一個問題，最早期儲存系統設計很少考量到隱私性的問題，大多將資料已明文儲存。後來安全議題被注意到，有許多分散式儲存系統將資料

加密後在儲存，其中所考量的攻擊者都是外來的入侵者，所以解密金鑰是由系統產生而且加解密都是由系統來進行。這類的分散式儲存系統大多皆使用加密系統來抵禦外來的攻擊。然而我們想要探討的資料隱私性，不僅是抵擋外來的攻擊，更要預防雲端儲存中的惡意主機。對使用者來說，全面相信雲端中的所有主機是較不實際的假設。如果能夠達到在使用者不用信任這些主機的情況下，仍能保障資料隱私性，這樣的保護機制與儲存系統才能真正被使用者信任。

資料的功能性是探討資料在被儲存到雲端後，雲端系統應該提供對於被儲存的資料的處理功能，例如關鍵字搜尋，全文搜尋，與儲存資料的個人存取控制與資料分享機制。使用者自己針對自己的儲存資料進行搜尋在應用密碼學上已有一些研究成果，例如支援關鍵字設定與關鍵字搜尋的加密系統，以及privacy preserving data mining技術。在全文檢索方面，目前有達到資料隱私性的研究成果是使用一個特殊的加密系統(fully homomorphic encryption)來對加密中的資料進行檢索運算，但是其效率不佳，尚無法實現於真實的系統中。

(2) 計算安全

當使用者將計算要求與參數傳送進雲端計算後，最終能夠得到雲端回傳的一個運算結果，但無法確認資料的運算是否正確。使用者自己重新計算一次在進行核對是一個直覺的作法，但是違反了雲端計算的精神。我們希望在雲端計算服務中，能夠提供使用者對計算結果的正確性進行確認。目前無論是學界或業界都鮮少有人注意到這個問題，亦鮮少有研究成果。

計算隱私性則是希望保障使用者的計算內容可以不被第三者得知，包括提供計算服務的雲端主機群也是。乍看之下會覺得這樣的假設很矛盾，既然希望由雲端來協助計算，又希望計算的內容不被洩漏，但在密碼學中的確有這樣的演算法存在，這類的研究稱為secure computation。然而在secure computation研究中，長年來無法克服的問題是針對不特定的運算程序，傳輸量一直都與計算程式本身成正比關係，也就是說當計算的程序越複雜，那麼使用者要上傳的資料量就越多。針對這個議題，fully homomorphic encryption是一個重要的研究，在本研究中我們的目標是了解其運作方式並進行在雲端中運用的實用性評估。

2. 研究成果

本計畫原提議為三年期計劃，但是核定下來的是兩年期，因此本計劃執行至第二年結束，這兩年完成工作內容分別說明於下。

（1）保護隱私的雲端偵測入侵系統

在本子系統中，我們用 Linux + Hadoop 來當作我們系統的平台，然後在這個平台上開發我們的雲端安全服務：Privacy-Preserving Cloud IDS. 而本系統分為兩大部分：使用者端和服務者端。使用者端是一個 java 程式，用來收集使用者電腦的資訊，經過隱私處理後，傳到雲端服務上做分析處理，在做最後的判斷，來判斷使用者的電腦是否安全無疑。服務者端採用 MapReduce 的程式架構來完成 hidden keyword search 的功能，用來比對使用者的上傳。除此之外，針對比對的資料庫，我們事先做好隱私處理，將這些資料放在 Datanode 上(HDFS)，用來做比對處理，目前系統已大致完成上述功能，期刊論文正在撰寫，近期將投稿。實做出的系統在下節介紹。

（2）雲端資料的存取控制

當資料儲存在雲端時，如何保障資料的隱私不被他人得知是重要的問題，資料加密是目前採用的方法。當資料是由多人使用，每個人有不同權限，要如何控管是我們研究的課題，我們可以想像資料分為幾個群組，群組之間有階層是的關係，當使用者可以存取高階層的資料時，他同時具有存取低階層資料的權限，反之則不行。

過去有許多相關的研究，但是解法都不太理想，我們發展了一系列的解決方法，利用密碼再加密的技術與金鑰推導的技術提出比之前改進的方法，特別是利用再加密技術得出的階層式金鑰設定與修訂的方法，不但可以讓雲端的計算量大幅降低，還可減少使用者的計算量，與更改金鑰時減少計算

量，這篇論文發表在高水準的 Infocom 2011 國際會議上，其餘的結果發表在 IEEE ANIA 2012 與 IEEE Trust-Com 2012 上

（3）非集中式雲端儲存系統中系統修復機制之研究

在雲端儲存系統中我們使用了容錯編碼來建構儲存系統的容錯能力，使用容錯編碼的儲存系統可以在系統中部分儲存伺服器無法提供服務時，維持整體儲存系統的對外資料存取服務。

經過我們對相關研究的資料收集與彙整後，我們發現現有的方法中，大多僅考慮一個儲存伺服器錯誤的狀況，並在錯誤發生後立即進行修復。有別於現有的方法，我們希望系統能夠先容許一小部份的伺服器錯誤，預測一個周期時間長度，進行周期性修復，以期避免經常執行大規模的修復動作。我們考慮當系統中有 x 個伺服器錯誤時，使用 x 個新的伺服器加入系統並進行修復動作。這些新的伺服器可以索取舊伺服器中儲存的資料並進行相關計算，最後儲存一個計算後的資料，一個修復後的儲存系統必須維持夠高的資料存取成功機率。

我們探討了系統中可以承受的錯誤比率，一個新伺服器需要詢問的舊伺服器數量，修復一個錯誤需要耗費的網路傳輸資料量，以及每個伺服器的儲存量。目前主要的發現是，考慮一個有 n 個伺服器的儲存系統，其中任意 k 個儲存伺服器可以協助使用者將資料取回。隨著系統中的伺服器發生錯誤，在系統中仍正常運作的伺服器數量若能維持在足夠的數量下，一個新的伺服器可以向少於 k 個舊伺服器索取資料，並修復一個伺服器錯誤造成的損失。這個成果發表在 IEEE Trust-Com 2011 國際會議上，期刊論文正在投稿中。

(4)資料完整性授權驗證

在本研究中，我們提出了可授權驗證的資料完整性檢查方法，進行驗證時不需下載完整的使用者資料，使用者也可以將驗證能力授權給信賴的代理人，進行授權的資料完整性驗證。我們提出的資料完整性授權驗證，包含以下三種角色：使用者（Data owner）、代理人（Delegated verifier）、以及儲存伺服器（Storage server）。我們的設計以私密驗證為基礎，利用額外的代理金鑰將使用者驗證標記，轉換為代理人所能驗證的標記，以達到授權驗證之目的。使用者對資料產生驗證使用的標記，並將資料及標記一併上傳至儲存伺服器，之後，也將代理人的代理金鑰送給儲存伺服器；代理人可對遠端伺服器進行資料完整性的驗證，藉由傳送挑戰值，儲存伺服器可利用代理金鑰產生對應的完整性證明，代理人將可利用自身的私密金鑰驗證回傳的完整性證明。在設計上，我們利用 bilinear map 進行 Tags 的轉換，儲存伺服器使用代理金鑰將使用者的 Tag 轉換為代理人的 Tag，代理人可對此 Tag 進行驗證。上述方法可支援同時授權多數的代理人，而不會造成使用者的計算負擔，以及儲存伺服器的儲存負擔，每增加一位代理人，系統上只會增加一把代理金鑰，使用者只需要利用自己的私密金鑰去產生代理金鑰，不需要去存取在儲存伺服器上的資料及代理金鑰，授權的動作將十分簡潔。這部分的成果發表在 ICICS 2011 的國際會議上。

3. 保護隱私的雲端入侵偵測

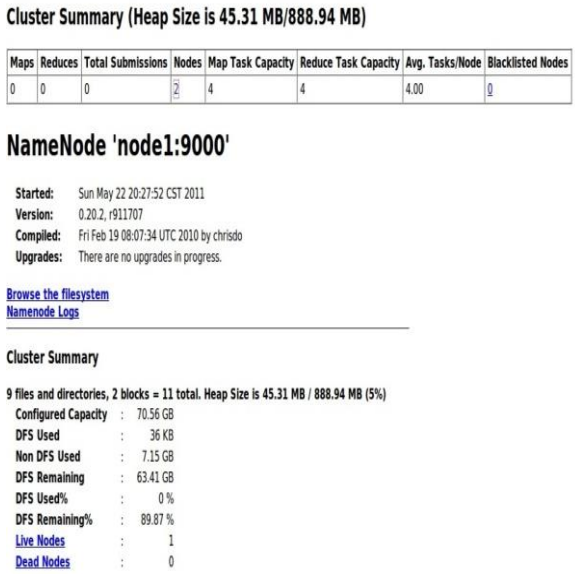
(1) **建立雲端環境**

本實驗中我們採用三台筆記型電腦當作我們的雲，每一台電腦是雙核心 1.4GHz，記憶體 2GB，硬碟 320GB，作業系統是 Ubuntu。安裝 Hadoop 來建立雲的環境，其中一台電腦為 Master，另外兩台為 Slaver。

在安裝 Hadoop 之前，要先將每一台電腦的網路給設定好。這個網路設定是為了確保每一台電腦可以正確的通訊，在本實驗中，我們將三台電腦分別設定為 192.168.0.161, 192.168.0.162, 192.168.0.164。可以利用"ping"或"telnet"來測試每一台電腦是否可以正確的通聯。因為 Hadoop 必須執行在 Java 虛擬機器上且版本必須為第 6 版以上，所以我們要安裝 Sun Java 6 的套件，可用 "apt-get install sun-java6-jre" 來完成 Java 的安裝。安裝完 Java 後，我們必須確認 Java 安裝的路徑，在

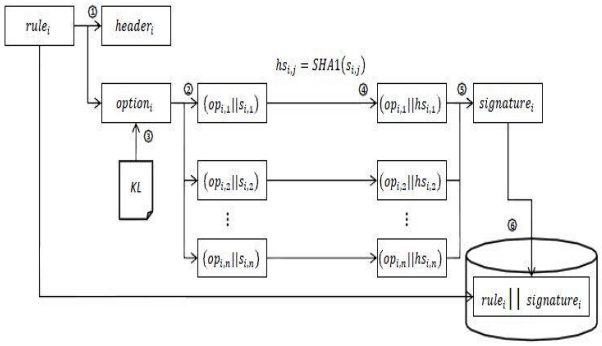
本實驗中為"/usr/lib/jvm/java-6-sun"，這個路徑是要用來設定 Hadoop 的設定檔，以確保 Hadoop 可以正確地找到 Java 安裝的位置。因為 Hadoop 是採用 SSH 當作每一個節點彼此的通訊方式，因此我們安裝 OpenSSH 以及設定每一個節點用來認證彼此的金鑰。安裝及設定完後可用"ssh ip"來確認安裝及設定是否成功。

完成好上述準備工作後(網路設定→安裝 Java→安裝設定 SSH)，接著我們才可以開始安裝 Hadoop。Hadoop 的安裝只要注意到其安裝的位置和使用者權限即可，在本實驗中我們的安裝路徑為"/opt/hadoop-0.20.2"(其版本為 0.20.2)，使用者為"hadoop"。安裝為後要設定 "hadoop-env.sh"、"core-site.xml"、"hdfs-site.xml"、"mapred-site.xml"、"master"、"slaver" 等相關檔案。完成其相關設定後我們可以開啟瀏覽器輸入：http://node1:50030 來檢查 Hadoop 是否可以運行。其運行圖如下圖所示。



(2) **建立關鍵字資料庫**

我們的入侵偵測服務是對電腦的網路封包做關鍵字比對，比對封包是否有和事先定義好的攻擊特徵符合。一個封包可以分為 header 和 payload 兩大部分，我們針對這兩部分做分析和比對，來檢查每一個封包內是否含有惡意的特徵值。因此，在 SNORT rule 當中，我們針對 Payload Detection 和 Non-payload Detection 兩大部分做分析和研究，希望可以找到最少組的關鍵字來做比對又可以涵蓋大部分的 SNORT rule。分析完 SNORT 規則後，我們選出三個關鍵字："content"、"flow"、"icode"當作關鍵字來轉換 SNORT 規則來成為我們的關鍵字資料庫。轉換的方法是保留上述所提到的關鍵字，加上述關鍵字的內容經過 SHA-1 固定長度後附加在原來規則的後方當作比對的關鍵字資料。最後我們將轉換後的關鍵字資料庫放到雲端上儲存。其轉換方法如下圖所示。



SNORT rule 中含有大約 8800 條左右的規則，而每一個 可分為兩部分，第一部分包括 SNORT rule 的行為、來源方 IP 和 PORT、接收方 IP 和 PORT、網路流向等部分，而第二部分是 SNORT rule 用來做比對的內容。而比對的部份我們只關心 Payload 和 Non-payload 的部分，所以我們將我們要比對的關鍵字做成 Keyword List (KL)來過濾分析內容。將取出的部分我們使用 SHA-1 雜湊函數來固定其長度和格式，當作是先定義好的特徵值。

(3) **保護隱私方法**

我們利用 Song, Wanger, Perrig 的方法和 Java 撰寫出對應的 client-server 程式來達到保護使用者上傳資訊的隱私。這個程式分為兩個部分：client 和 server。

Client 這程式具有以下能力：收集使用者電腦的封包、分析和轉換收集來的封包、加密收集來的封包、儲存收集來的封包、上傳資訊到雲端、比對候選者名單和儲存收集過的封包來判斷是否遭受惡意攻擊。

目前這個程式只支援在一般電腦上執行。使用該電腦的使用者必須擁有 root 以上

的執行能力(為了打開網卡收集封包)且該電腦必須安裝 jpcap 這個 library(支援收集封包的 library，該 library 目前不支援 64bit 的作業系統)和 Sun-Java(執行 Java 程式)。接著在一般電腦上執行"sudo java client"，即可開始執行上述功能。執行畫面如下圖所示。

下圖為收集封包示意圖

下圖為封包加密上傳示意圖

Server 這程式具有以下能力：讀取和儲存關鍵資料庫、做關鍵字比對來分析上傳的封包是否為可能的惡意攻擊、回傳候選者名單給使用者做最後的判斷。

Server 在收到 client 的 request 時，Server 會先將收到的 request 做一個前置處理，這個處理主要是要取出從 client 端傳來封包的時間序號，我們將這個時間序號當作 index 來識別每一個上傳的封包；接著我們將其他上傳的資訊寫入一個檔案裡面，用這個 index 當作檔名，上傳到 Hadoop 的 HDFS 上面

"Process p = run.exec("/opt/hadoop-0.20.2/bin/hadoop dfs -moveFromLocal " + name + " ."); "

最後我們在 Hadoop 上寫一個 www 的程式來做關鍵字比對的功能，當 Server 收到 client 的 request 時，就會去執行 www 這個程式來完成關鍵字比對的工作。www 這個程式的功能是讀取和儲存關鍵資料庫以及做關鍵字比對且 使用 Hadoop 自動地將工作分配給 slaver 這些 nodes 去執行。首先 www 要先找到儲存在 HDFS 上的關鍵字資料庫

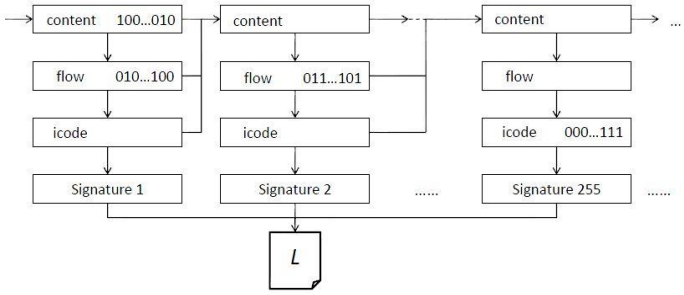
"FileInputFormat.setInputPaths(conf, new Path("/user/hadoop/sig")); "，接著取出其內容" map(LongWritable key, Text value, OutputCollector<Text, IntWritable> output, Reporter reporter) "，" String line = value.toString(); "

另一方面，我們還必須將前面所提到的 index 這個檔案從 HDFS 中找出來

" patternsFiles =DistributedCache.getLocalCacheFiles(job); "，

" BufferedReader fis = new BufferedReader(new FileReader(patternsFile.toString())); "

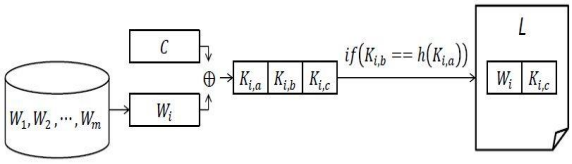
找出來之後我們利用下面流程來和關鍵字資料庫的資料做比對如下圖所示。



我們將從關鍵字資料庫取出來的資料稱作 $data_i = rule_i||signature_i$，而 index 這個檔案裡個資料稱作 packet。其中 $signature_i$ 要和 packet 做比對，當比對正確時，我們才會將 $rule_i$ 放到候選者名單 L 中，當作回答傳回給使用者。每一個 $signature_i$ 和 packet 都會含有"content"，"flow"，"icode"這三個關鍵字，比較的內容是關鍵字後面的那一串二進位的值，其比對的流程是先比"content"，若正確則往下比"flow"，若依然正確則繼續往下比"icode"，反之一旦失敗，則比下一條 $data_i$。若關鍵字後面沒有那一串二進位的值，則當作正確，繼續比下一個關鍵字。

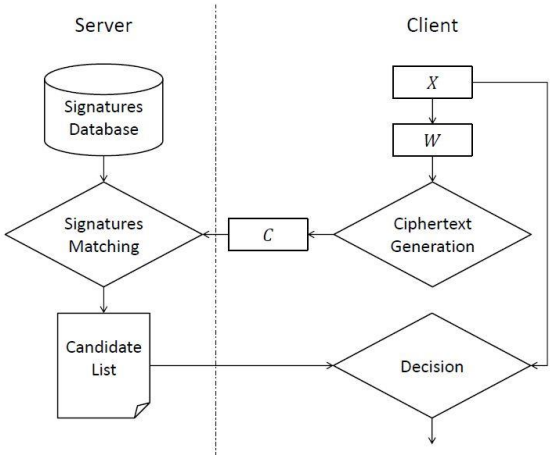
接著我們將說明比對的方法為何，在這我們會說明上述所提到的正確和失敗，何謂比對正確？何謂比對失敗？其關鍵字比對方法如下圖所示。首先先比對 $signature_i$ 和 $data_i$ 關鍵字為 content 的部分，將這兩部分後面那一串二進位的值做 xor 的運算，會得到一個 Ki=Ki,a||Ki,b||Ki,c 的值，假設 h(Ki,a) 前面的 s bits 和 Ki,b 的值一樣，則判斷為正

確，反之則判斷為錯誤。將判斷正確的 rulei 和 Ki,c 放到候選者名單 L 中。



目前這個 Server 程式會將收到的 Client 的 request 上傳到 Hadoop 的 HDFS 上，然後再去執行在 Hadoop 上的 www 這隻程式，當 www 程式執行完畢將結果留在 Hadoop 的 HDFS 上時，Server 才去將結果給取回來，回傳給對應的 Client 端。

藉由前面雲端環境的建立和關鍵字資料庫的建立，此 client-server 程式根據 Song, Wanger, Perrig 的方法來完成保護隱私的功能，其正確執行流程如下圖所示。首先 Client 會收集封包 X，經過分析和轉換後將其長度固定為 W，利用 Chiphertext Generation 這步驟將 W 加密為 C 上傳到 Server；Server 處理收到的 C 後，經過 Signatures Matching 去比對 C 和 Signatures Database，若有符合的則放到 Candidate List 傳回給 Client；最後 Client 收到 Candidate List 後經過 Decision 的步驟盼端先前上傳的封包是否為一個惡意的攻擊。



4. 計畫成果自評

這兩年 (NSC-99-2218-E009-020 ，NSC-100-2218-009-006) 我們的研究成果發表了以下的相關論文:

（1） Yi-Ruei Chen, J.D. Tygar, W.-G. Tzeng, Secure Group Key Management Using Uni-Directional Proxy Re-Encryption Schemes, In the 30th IEEE International Conference on Computer Communications (INFOCOM 2011), April, 2011.

（2） Shiuan-Tzuo Shen, Wen-Guey Tzeng. Delegable Provable Data Possession for Remote Data in the Clouds. In the 13th International Conference on Information and Communications Security (ICICS 2011), Nov, 2011.

（3） Hsiao-Ying Lin, Wen-Guey Tzeng, Bao-Shuh Lin. A Decentralized Repair Mechanism for Decentralized Erasure Code based Storage Systems. In the10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-2011), Nov, 2011.

（4） Hsiao-Ying Lin, Wen-Guey Tzeng, Shiuan-Tzuo Shen and Bao-Shuh P. Lin. A Practical Smart Metering System Supporting Privacy Preserving Billing and Load Monitoring. In the10th International Conference on Applied Cryptography and Network Security (ACNS 2012), June, 2012.

（5） Hsiao-Ying Lin, Shiuan-Tuzo Shen, Wen-Guey Tzeng, Bao-Shuh Lin. Toward Data Confidentiality via Integrating Hybrid Encryption Schemes and HDFS. In the 26th IEEE International Conference on Advanced Information Networking, (IEEE AINA 2012), March, 2012.

（6） Yi-Ruei Chen, Wen-Guey Tzeng. Efficient and Provably-Secure Group Key Management Schemes Using Key Derivation.In the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-2012), June, 2012.

以論文成果來看，第一篇在 Infocom 2011 的論文為高水準的會議論文，其餘的論文亦達中上的水準。我們還正將其改寫為期刊論文，投稿到知名的國際學術期刊。

雖然計劃被刪為兩年，我麼還是實做出系統來。從論文成果及實做的成果來看，我們達成的計劃預期的目標。

參考文獻:_

[1] Zooko Wilcox-O'Hearn and Brian Warner. "Tahoe: the least-authority fileystem." ACM international workshop on Storage security and survivability – StorageSS 2008, pages 21-26, 2008.

[2] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano,"Public key encryption with keyword search"Annual international Cryptology Conference on Advances in Cryptology – EuroCrypto 2004, pages 506-522, 2004.

[3] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters,"Attribute-based encryption for fine-grained access control of encrypted data", ACM Conference on Computer and Communications Security – CCS 2006, pages 89-98, 2006.

[4] John Bethencourt, Amit Sahai, Brent Waters."Ciphertext-Policy Attribute-Based Encryption." IEEE Symposium on Security and Privacy, pages 321-334, 2007.

[5] Rafail Ostrovsky, Amit Sahai, Brent Waters." Attribute-based encryption with non-monotonic access structures." ACM Conference on Computer and Communications Security – CCS 2007, pages 195-203, 2007.

[6] Lea Kissner and Dawn Xiaodong Song. "Privacy-Preserving Set Operations." Annual international Cryptology Conference on Advances in Cryptology – CRYPTO 2005, pages 241-257, 2005.

[7] Jaideep Vaidya and Christopher W. Clifton. "Privacy-Preserving Kth Element Score over Vertically Partitioned."IEEE Transactions on Knowledge and Data Engineering." 21(2):253-258,2009.

[8] Yingpeng Sang and Hong Shen. "Efficient and secure protocols for privacy-preserving set operations." ACM Transactions on Information and System Security." 13(1), 2009.

[9] Ari Juels, Burton S. Kaliski Jr.," PORs: Proofs of Retrievability for Large Files." ACM Conference on Computer and Communication Security – CCS 2007, pages 297-306, 2007.

[10] Hovav Shacham and Brent Waters. "Compact proofs of retrievability." The 14th international Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 2008, pages 90-107, 2008.

[11] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, Dawn Song,"Provable Data Possession at Untrusted Stores." ACM Conference on Computer and Communication Security – CCS 2007, pages 598-609, 2007.

[12] Giuseppe Ateniese, Seny Kamara, Jonathan Katz, "Proofs of Storage from Homomorphic Identification Protocols." The 15th International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 2009, pages 319-333, 2009.

[13] Kevin D. Bowers, Ari Juels, and Alina Oprea "HAIL: a high-availability and integrity layer for cloud Storage." ACM Conference on Computer and Communications Security – CCS 2009, pages 187-198, 2009.

[14] Qian Wang, Cong Wang, Jin Lin,Kui Ren,Wenjing Lou." Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing." The 14th European Symposium on Research in Computer Security – ESORICS 2009, Pages 355-370, 2009.

[15] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou." Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing." IEEE international conference on computer communications - INFOCOM 2010, 2010.

[16] Andrew Chi-Chih Yao." Protocols for Secure Computations." IEEE 23rd Annual Symposium on Foundations of Computer Science – FOCS 1982, pages 160-164, 1982.

[17] Server Protectors LLC, Secure cloud storage, http://serverprotectors.com/solutions/secs

[18] Craig Gentry. "Fully homomorphic encryption using ideal lattices." The 41st annual ACM symposium on Theory of Computing – STOC 2009, pages 169-178, 2009.

[19] Marten van Dijk, Craig Gentry, SHai Halevi, and Vinod Vaikuntanathan. "Fully homomorphic encryption over integers." Cryptology ePrint Archive, Report 2009/616, 2009.

[20] N. P. Smart and F. Vercauteren. "Fully homomorphic encryption with relatively small key and ciphertext sizes." Cryptology ePrint Archive, Report 2009/571, 2009.

國科會補助計畫衍生研發成果推廣資料表

日期:2012/11/01

國科會補助計畫	計畫名稱: 子計畫一：支援多樣功能之雲端資料安全儲存(2/2)
	計畫主持人: 曾文貴
	計畫編號: 100-2218-E-009-006- 學門領域: 資訊

無研發成果推廣資料

100 年度專題研究計畫研究成果彙整表

計畫主持人：曾文貴	計畫編號：100-2218-E-009-006-
計畫名稱：前瞻性雲端安全儲存、防護、行為分析與觀測平台--子計畫一：支援多樣功能之雲端資料安全儲存(2/2)	

成果項目			量化			單位	備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等）
			實際已達成數（被接受或已發表）	預期總達成數(含實際已達成數)	本計畫實際貢獻百分比		
國內	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	0	0	100%		
		專書	0	0	100%		
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（本國籍）	碩士生	3	0	100%	人次	
		博士生	1	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		
國外	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	6	0	100%		
		專書	0	0	100%	章/本	
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（外國籍）	碩士生	0	0	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		

其他成果 (無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。)	發展雛形系統，已用 open foundry 的系統上傳。

	成果項目	量化	名稱或內容性質簡述
科教處計畫加填項目	測驗工具(含質性與量性)	0	
	課程/模組	0	
	電腦及網路系統或工具	0	
	教材	0	
	舉辦之活動/競賽	0	
	研討會/工作坊	0	
	電子報、網站	0	
	計畫成果推廣之參與（閱聽）人數	0	

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■達成目標

□未達成目標（請說明，以 100 字為限）

□實驗失敗

□因故實驗中斷

□其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文：■已發表 □未發表之文稿 □撰寫中 □無

專利：□已獲得 □申請中 ■無

技轉：□已技轉 □洽談中 ■無

其他：(以 100 字為限)

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）(以 500 字為限)

（1）本計劃（兩年期）發表 6 篇會議論文，其中有高水準的 Infocom 國際會議論文，其餘論文的水準都屬中上，期刊論文正在撰寫投稿中。

（2）發展雛形系統。

（3）培養學生投入我國的 IT 產業，促進國家的經濟發展。