Communications of the CCISA
Vol. 24 No. 3 Jul. 2018

雲端外儲系統資料保護機制

黃仁俊 [1*]、張軒齊 [2]
[1, 2] 淡江大學資訊工程學系
[1]victor@gms.tku.edu.tw、[2]peter30622@gmail.com

摘要

雲端計算的諸多優點吸引企業組織和個人將其資料由自行管理的傳統模式逐漸轉變為託管儲存在遠處的雲端伺服端，尤其雲端用戶可以將大量資料及相關管理與維護的工作負荷託管轉嫁給雲端伺服端，並以依用多少付多少的標準支付費用的形式使用近似毫無限制的資源。然而無可避免地，雲端用戶的儲存資料可能具機敏性，因此保護儲存資料的私密性與處理過程中隱私性的確保將成為雲端計算服務推展成功與否的重要關鍵。資料加密後再上傳到雲端伺服端是保護資料私密性最根本的做法，本研究設計並實作資料儲存於雲端儲存系統的安全技術，研發設計資料上傳與下載的安全機制，該機制提供的功能(1)資料上傳與下載過程資料私密性與完整性；(2)儲存於雲端儲存系統資料私密性與完整性；與(3)有效率的偵測錯誤資料區塊與資料復原功能。同時本研究亦以程式實現此安全機制於手機平台 google 與 amazon 提供雲端平台，本研究成果使儲存於雲端儲存系統的資料的安全性掌握在資料擁有者手中，無論雲端儲存服務提供的安全機能如何，讓儲存資料受到保護的程度都在資料擁有者所能控制的範圍內，讓資料因安全性問題可能造成的傷害或損失降到最低，而且整個機制的運作就在資料擁有者個人的手機平台上。本研究成果對雲端服務的推廣應有顯著的助益。

關鍵詞：雲端運算、雲端儲存、資料安全

The Data Protection Mechanism of Cloud Outsource Storage

Ren Junn Hwang [1*], Hsuan Chi Chang [2]
[1, 2] Department of Computer Science and Information Engineering, Tamkang University
[1]victor@gms.tku.edu.tw, [2]peter30622@gmail.com

Abstract

Cloud outsource storage has many advantages that attract many business organizations and individuals to store their data in a remote cloud storage. The cloud users transfer large amounts of data and maintenance workloads to cloud servers, and to use seemingly unlimited resources. There are sensitive data stored in the outsource storage. To protect the privacy of the stored

* 通訊作者 (Corresponding author.)

data and to ensure the confidentiality of the processing will be the key to the success of cloud computing services. Data encryption and then upload to the cloud storage is the most fundamental protection of data privacy. This paper designs and studies the security technology of the data stored in the cloud storage. The proposed mechanism provides: (1) Data privacy and completeness of data upload and download processes. (2) Protect the privacy and integrity of the data stored in the cloud storage. (3) To detect and recover the error data blocks efficiently. The data owners perform the proposed protection processes (software) and upload the protected data to cloud outsource storage. The entire security processes are operated by the owner himself on his mobile platform. The extent to which stored data is protected is within the control of the data owner. This strategy minimizes the damage or loss caused by security problems. The research results will promote the cloud storage application services.

Keywords: Cloud computing, Cloud storage, Data security

壹、前言

隨著行動通訊相關機制與技術的成熟，手機幾乎是每個人隨身的必備用品，由於手機的便利性與行動網路通訊的普及，幾乎隨時隨地在世界任何有網路的地方都能夠上網，且手機的功能越來越強大，各式的通訊軟體、遊戲、上網功能以及生活上的小工具等包羅萬象的許多功能使得我們可以透過手機來完成工作與日常生活許許多多的大小事情；放眼望去在我們的生活周遭，不論是在街道上的行人、在學校上課的學生，乃至於在家中小孩的娛樂，大部分都有手機身影，大家一有空閒就“滑”手機，手機的普及性已是無庸置疑的，甚至已深深融入我們的日常生活當中，未來有可能變成生活必需品，網路通訊也極有可能成為有如現在的水與電一樣重要，成為民眾工作與日常作息的基本必需品。

手機的可攜帶性高，常常只要放進褲子的口袋中，就能隨身帶著走，一有需求就能立刻拿出來使用，非常方便，因此外機體設計講究的是輕、薄、短、小，手機再大也不過和我們的手掌一樣大，體積小的訴求自然地導致手機內部儲存空間受到某種程度的限制，手機的資料或軟體的儲存空間無疑地因為隨著機體體積的限縮而受到限制，但是因為手機的錄音、相機、攝影或筆記本軟體的發達與便利，手機持有者透過手機產生數位資料量卻反向的大幅資加，因此雲端應用中的雲端儲存服務就變成是手機各項應用服務中非常重要而現在也非常普及的一項服務，尤其透過雲端儲存也能使手機輕易地與其他計算平台如桌上型電腦分享彼此的資料。

雲端儲存服務現在也被越來越多人作為取代傳統隨身碟工具，而隨身碟必須隨時攜

帶在身上，以防不時之需，其實並不怎麼方便，一不小心遺失還有資料外洩及資料遺失之風險，而隨身碟因外力毀損也可能造資料毀損，取而代之的是只要上傳到雲端儲存系統，只要雲端儲存服務的安全機制夠健全，雲端儲存不但可以改善隨身碟的全部缺失，還可以增加便利性同時也將低成本，不過必須有健全安全儲存機制來支持，藉以確保資料完整性與保護私密和隱私，否則造成的傷害可能非常的大後果不堪設想。

雲端計算環境為一集中控管並有效率調配資源且透過普及的網路通訊技術以提供低成本與高便利性應用服務系統，在軟體即服務(SaaS)中，存在許多誘人的優勢[6]，首先,使用者不需要擁有一個自己的資料中心(data center),也完全不需要對其管理及維護,統一由雲端服務供應商控管，設備的購置、維護與人力成本全部都節省下來，也不必擔心系統軟體版本升級與硬體機器老舊的問題；再者，雲端計算或是儲存對於 IT 資源的使用皆具擴充性(scalability)與彈性，並根據使用者使用資源的多寡自動調整，更重要的是使用者只根據使用的量支付費用(pay on demand)，讓成本費用降低並貼近實際需求；最後，雲端服務提供應用程式之間設備獨立的特性，支援災害復原(disaster recovery)及業務的連續性(business continuity)。以上種種雲端的優點，都再再顯示雲端即將是未來一個普遍的運作模式。

雲端計算固然帶來許多好處，但也帶來不少隱憂，其中又以安全功能的健全與否令人憂心，也成為決定採用雲端服務的重要關鍵因素之一，雲端計算聯盟(CSA)曾公布雲端計算的安全威脅，其中與資料儲存於雲端儲存系統相關的有資料洩露、資料遺失、與惡意的內部員工等。CSA 認為資料洩露，採取加密技術可能是可以緩解此種威脅，同時使用者對資料加密，也減小洩露的風險包括惡意內部員工的偷窺，不過卻會衍生另一種威脅即一旦遺失了加密金鑰，資料則再也無法挽回如同毀損或遺失。CSA 認為第二項資料遺失，帶來的問題不僅會影響雲端供應商與企業用戶的信任關係，依照法規，企業用戶必須儲存某些資料檔案達一定的法定年限以備相關稽政單位包括政府部門的核查，但這些資料一旦遺失，企業用戶可能因此陷入困境，遭到政府的懲罰。此外，雲端儲存服務也存在另一問題即資料確實刪除與否的問題，資料擁有者透過平台刪除其在雲端儲存系統的特定檔案之後，該檔案可能因為雲端儲存服務供應商內部的檔案管理機制或備份機制的因素，實質上資料尚留存於服務供應商的實體系統，只是一般使用者包括資料擁有者無法存取而已，這對資料擁有者私密性或隱私還是構成威脅。許多企業更明確指出雲端計算之資安議題是雲端計算服務最嚴重的挑戰，而這也是他們考量是否將資料移植到雲端儲存系統決策過程一項極關鍵參考指標。

一般人在選擇或使用雲端儲存服務時，優先考慮的往往是它的儲存空間有多大、使用介面是否便利，卻忽略了雲端儲存服務潛在的安全隱憂。使用者也許認為雲端技術相當成熟，所以放心地把一些重要或私密的檔案和資料放在雲端上，但事實上這可能還是防不住有心入侵的駭客，駭客發動網路攻擊輕而易舉、恣意妄為，透過網路垃圾製造者及惡意程式碼的行為，即可輕易地運用雲端平台來發動阻斷式服務攻擊，進行密碼的破解或其他病毒式軟體來影響其他合法的租用者，甚至有些雲端服務供應商在提供給使用

者短期試用時，網路駭客也會以匿名者進行雲端平台犯罪行為，所以雲端公司如何保護雲端的資料不被外來的駭客攻擊是一個很重要的議題；也可以換一個角度來思考，雲端使用者所選用的雲端服務供應商對使用者的資料內容來說不也是 “外來的”個體嗎？雲端服務供應商內部員工可以輕易地“接近”我們寄存的資料。舉例而言， Google 公司 2012 年在他們與用戶的雲端儲存使用條款中寫道：「當你將資料上傳或用其他方式提交到 Google Drive 後，你就給予 Google（以及我們的合作夥伴）全球授權，可以使用、代管、儲存、再製、修改、建立衍生內容、溝通、出版、公開呈現、和遞送這些內容。」隱私保護團體對此也提出強烈質疑，甚至有人表示，Google 已經擁有使用者的許多個人資料，Google Drive 意味著 Google 可以掌握更多資料。從這則 2012 年的報導，我們很快地就能理解其實就連本身提供雲端儲存服務的公司都不一定如我們想像的安全可靠；全球知名而為大家所熟悉的 Google 或 Dropbox 是否真能提供安全機制達我們想像的程度，都是要存疑的，所以如果直接將重要或隱私的資料上傳至雲端，即有可能就會發生像是 2014 年 8 月 31 日晚間在美國的 Reddit、4chan 網站流出大量好萊塢女星的私密照片一樣，造成個人或企業極大傷害或影響。

對於雲端儲存服務的安全性、儲存系統的安全管理與提供雲端服務的公司可信度，我們無法十足掌握，就像是資料寄存在別人的系統受其管控，隨時有被偷窺和竄改的威脅，我們難以時時監控，再加上雲端服務供應商之資訊技術能力遠勝於一般使用者或企業，在種種不對稱的因素之下，雲端儲存服務實質上似乎變成了只提供儲存功能但卻不一定安全的服務。一般的社會大眾如果沒有具備資訊安全的知識，單純地認為雲端十分可靠，於是便把所有重要或具隱私性的資料存放到雲端上，還非常慶幸原來有這麼好的服務可使用，卻沒意識到自己已曝露在一些資安風險中，假以時日可能造成無法挽回的傷害或損失還不自知。

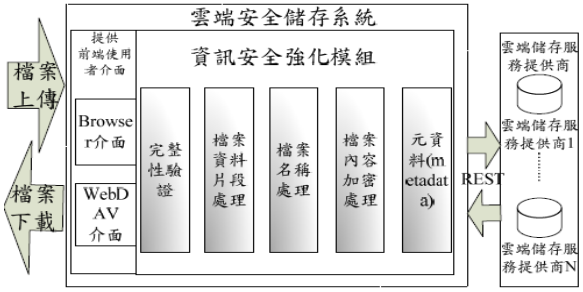
使用者一經選擇使用雲端儲存服務，無法實質改變或要求供應商對雲端儲存服務的安全機制，也無法改變雲端儲存服務各項安全功能，但雲端儲存服務搭配手機與行動網路後為使用者帶來的便利性與行事效率非常吸引人也無庸置疑；有鑑於此，本論文研究並實作資料儲存於雲端儲存系統的安全技術，研發設計一手機應用軟體讓使用者自力更生地將儲存於雲端儲存系統的資料的安全性掌握在自己手中，無論雲端儲存服務提供的安全機能如何，讓儲存資料受到保護的程度都在我們所能控制的範圍內或讓資料因安全性問題可能造成的傷害或損失降到最低，而且整個安全機制的運作就在我們個人的手機平台上。

貳、文獻探討

近幾年來有很多文獻討論雲端的儲存系統運作與應用的安全議題，但就實務面並實際建置成可運作的軟體來看與本論文最直接相關的當屬中華電信研究院的雲端安全儲

存系統[9]。該院提出的解決方案在使用者與雲端供應商之間建立一名為雲端安全儲存系統，協助使用者或企業組織解決資料儲存於雲端儲存服務供應商的安全問題，圖一是該院發布的雲端安全儲存系統使用情境示意圖，圖二為雲端安全儲存系統架構圖。該院的雲端安全儲存系統建立完整性驗證、檔案資料片段處理、檔案名稱處理、檔案內容加密處理與建立元資料(MetatData)檔案等五個程序處理使用者傳送來預計上傳到雲端儲存服務供應商的資料後，再透過 REST 協定傳送至後端各種支援 S3 Compatible 的雲端儲存服務供應商的系統，由於各個上傳完成的檔案已經過雲端安全儲存系統做資訊安全安全強化處理，所以終端的雲端儲存服務供應商無法得知實際檔案資料的內容。

圖一：雲端安全儲存系統使用情境示意圖[9]



圖二：雲端安全儲存系統架構圖[9]

中華電信研究院雲端安全儲存系統所支援的系統種類很多，不論是在手機、電腦甚至虛擬機都可以運行，介面十分人性化、友善性高，整個版面配置看起來非常舒適，功能也非常多元，適合企業組織選用後，透過雲端安全儲存系統同步控制各個部門或員工對資料的存取權限，十分方便，但就個人戶的使用者而言存在以下議題值得深入探討或再求進步甚至改善的空間。

1.只適合企業組織

就該系統公開的文獻資料可以理解就使用者端而言資料都是原有的面貌呈現，執行資料保護的機制與程序是另一獨立的雲端安全儲存系統，非使用者端使用的計算平台，

個人使用者或小型工作室可能沒有能力建立或採購此系統，因此該系統適合較具規模的企業組織，一般個人使用者或小型工作室並不適用。

2.金鑰管理機制

金鑰管理是資訊安全系統非常重要的基石，所有的密碼技術安全性能再怎麼強健沒有安全的金鑰管理機制支援，還是形同虛設，該系統公開的文獻資料並沒有說明金鑰管理機制的作法，當然因該系統情境的安全機制與運作是建立在雲端安全儲存系統中，使用者沒有實質的運作，因此公開的文獻資料並沒有說明金鑰管理是可以理解的，但若一般使用者沒有有效率金鑰管理機制支援，安全保護機制的機能恐怕會功虧一簣。

3.有效率的支援資料異動

檔案上傳儲存到雲端儲存服務系統後，資料擁有者不免會有異動該檔案資料的需求，該系統公開的文獻資料，並沒有討論使用者異動檔案資料內容時，雲端安全儲存系統如何有效率的異動雲端儲存服務系統所儲存的資料。然而，資料異動是使用者使用檔案資料必然存在的功能。

4.辨識錯誤資料的區間

檔案上傳到雲端儲存服務系統後，會被切割分區塊儲存於實際的硬碟系統中，然而當資料完整性驗證出現問題時，是否能有效率的偵測出錯誤的區塊是值得重視的議題，因為精確的判斷錯誤區塊的位置，不但可以讓使用者繼續引用正確區塊資料，以降低使用者因資料毀損所造成的損失，也可以使錯誤資料的救援工作更有效率或救援成本也會降低，但該系統公開的文獻資料並沒有討論此一議題。

5.資料復原

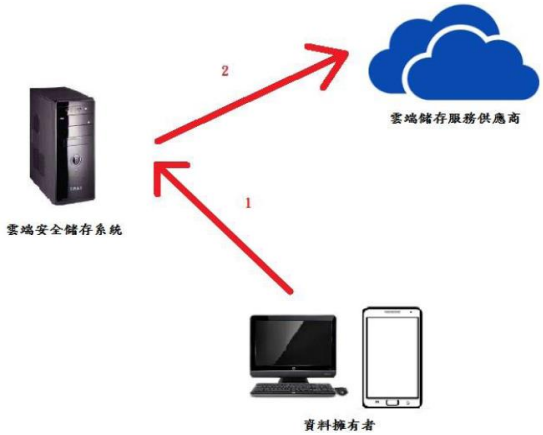
就該系統公開的文獻資料沒有說明資料儲存於雲端儲存服務系統後，如果資料遺失、竄改或錯誤後如何復原的問題，雖然在其雲端安全儲存系統存在資料完整性驗證機制，但如果資料完整性出現問題如何進行資料復原工作使不容忽視的議題，一般而言，資料上傳寄存於雲端儲存服務系統後，使用者不會留存原始資料，否則就不必選用雲端儲存服務，但若只發現資料不正確，卻也無法復原，對使用者而言傷害與損失還是存在，最多只能避免其引用錯誤資料而已，在安全機能上有進步空間。

參、本論文方法

本論文研究並實作資料儲存於雲端儲存系統的安全技術，資料擁有者透過本論文研發設計的手機應用軟體可以將儲存於雲端儲存系統的資料的安全性掌握在自己手中，無論雲端儲存服務提供的安全機能如何，讓儲存資料受到保護的程度都控制在一定的範圍內或讓資料因安全性問題可能造成的傷害或損失降到最低，很重要的是整個安全機制的運作就在資料擁有者個人的手機平台上，安全機能的運作不假手其他系統，除了雲端儲存服務供應商提供實體儲存服務之支援外，本論文研展的系統無須其他系統的支援。圖

三與圖四分別是本論文研究之系統應用情境與中華電信研究院之雲端儲存安全系統情境在簡化後的示意圖，透過簡易示意圖的比較很明顯地呈現兩者間的差異，尤其是本研究開發之機制在資料擁有者與雲端儲存服務供應商間無第三系統介入其中。不僅如此，本研究開發之機制不但提供類似中華電信研究院雲端儲存安全系統大部分安全功能，也針對本論第貳節討論中華電信研究院雲端儲存安全系統可以再進一步提升的議題，研究發展解決方案並實作。下列說明本論文研擬的研究方法與方向，其中也包括本論文研展過程會採用的密碼技術，而本論文技術與中華電信研究院雲端儲存安全系統同樣達成的安全功能，就不再進一步說明。

圖三：本論文運作之系統情境示意圖



圖四：中華電信研究院雲端儲存安全系統情境示意圖[9]

3.1 系統架構

本論文探討之整體系統環境如圖五系統架構。開發之 APP 執行後將進入如圖六之登入畫面，使用者第一次啟動此 APP 需選擇 “APP 首次登入” 功能以建立後續使用 APP 所需之密碼。密碼建置完成後，使用者登入輸入密碼後按 “確認” 進入圖七主畫面。

圖五：系統架構圖

圖六：手機登入畫面

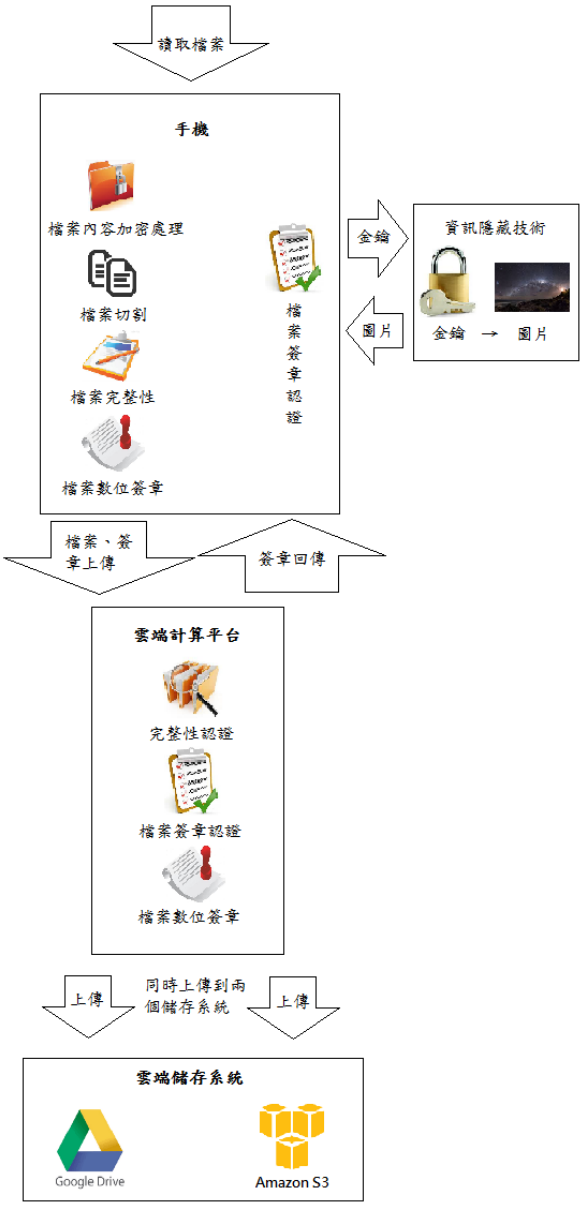
使用者第一次使用本論文設計之軟體需在圖七主畫面按選 “註冊” 功能，完成各種金鑰與參數之設定並自雲端 GAE 計算平台取得相關參數。註冊完成後，雲端 GAE 計算平台持有手機之公鑰；手機將持有自己的私鑰與雲端 GAE 計算平台之公鑰，作為後續執行簽章或驗簽章之憑藉。在此註冊程序本論文設計以橢圓曲線密碼技術為基礎的金鑰，

而各平台將自行產生各自之私鑰與公鑰。

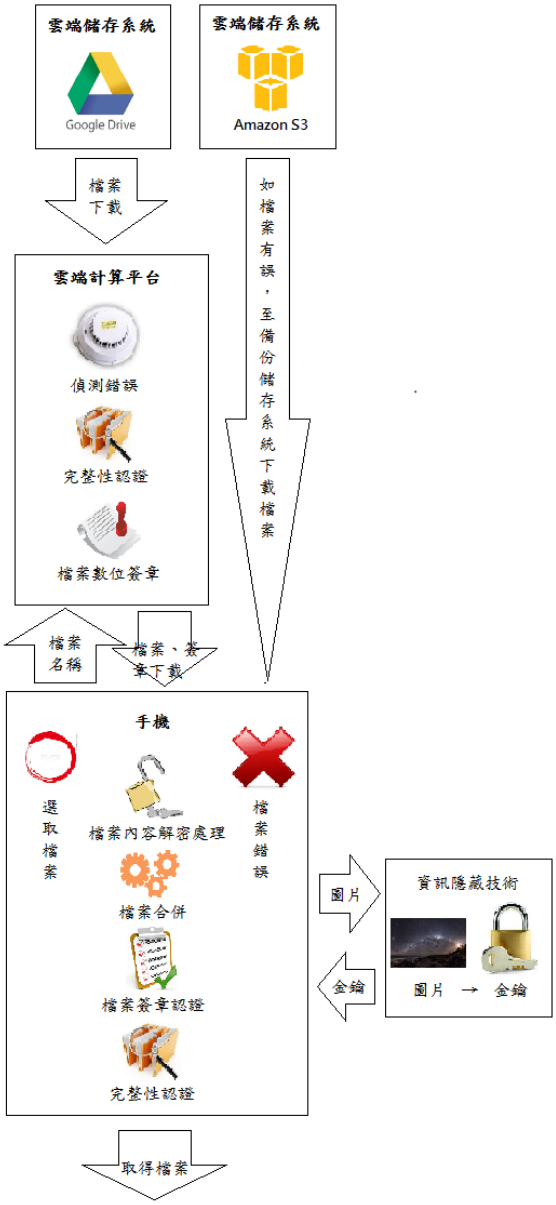
圖七：手機程式主畫面

在圖七主畫面按選“上傳”功能將執行圖八的上傳處理程序，檔案在手機端以 XTS-AES 模式加密切割並以橢圓曲線數位簽章後分送 google GAE 計算平台，GAE 計算平台完成確認程序後，存入 google cloud storage 儲存系統，以及將檔案發送至 amazon EC2 計算平台，EC2 計算平台完成確認。GAE 與 EC2 各自進行本論文以 Java 語言設計之 Hash Tree 和 ECC 數位簽章為基礎確認程序，包括驗證儲存資料之完整性，確保資料在傳遞過程未遭不當的增刪與異動，同時也驗證簽章確認資料來源為資料擁有者，另外，儲存資料是以密文形式進行前述檢驗，而儲存在雲端儲存系統也始終維持密文檔形式以確保私密性。

在圖七主畫面選擇“下載”功能將執行圖九的下載處理程序，google GAE 計算平台雲端儲存系統根據使用者之指定取得檔案進行檔案正確性之檢視後傳送給手機，手機檢視檔案正確性，若沒有錯誤自密鑰圖像取出密鑰後以 XTS-AES[8]模式解密檔案還原原始檔案；若部分檔案區塊有錯誤，自 Amazon S3 雲端儲存系統取得對應的檔案區塊，再自密鑰圖像取出密鑰後解密檔案還原原始檔案。後續子節，本報告進一步說明本論文使用與開發和安全相關的技術。


讀取檔案
手機
檔案內容加密處理
檔案切割
檔案完整性
檔案數位簽章
檔案簽章認證
金鑰
圖片
資訊隱藏技術
金鑰 → 圖片
檔案、簽章上傳
簽章回傳
雲端計算平台
完整性認證
檔案簽章認證
檔案數位簽章
上傳
同時上傳到兩個儲存系統
上傳
雲端儲存系統
Google Drive
Amazon S3

圖八：上傳程序示意圖



圖九：下載程序示意圖

3.2 檔案切割區塊處理

資料擁有者上傳儲存到雲端儲存服務供應商的檔案將切割成幾個區塊，亦可視為子檔案，經安全處理程序後再上傳[5]。每個子檔案區塊大小本論文考量以 TCP/IP 一個封包 payload 所能承載的資料量大小為考量的根據，因為資料檔案透過 TCP/IP 傳送時，其資料量達到一定程度後，縱使在資料應用層沒有切割但到下層的傳輸層也會強制切割，分成多個封包遞送到目的端。本論文考量 TCP/IP 一個封包 payload 所能承載的資料量大小做為切割後子檔大小的根據，在實務面不會因本論文將檔案切割成子檔的運作模式造成資料擁有者存取雲端資料所需的通訊成本太多的額外負擔，經此先行切割後就資料本

身而言是幾乎沒有增加額外的通訊成本，因為沒有採行本論文安全機制時，本來的檔案就切割成相同數量的封包來傳送。

3.3 HMAC (Keyed-hash message authentication code)

本論文採用 HMAC[1]作為驗證資料完整性的核心技術，我們採用 SHA256 嵌入 HMAC 運作機制有效率的快速產生各個階段的訊息鑑別碼(Message Authentication Codes，MAC)，使得資料完整性的機能以及偵測錯誤區塊子檔的目標可以有效率的實現。

3.4 應用 Complete Binary Tree 在資料錯誤的偵測上

本論文結合 HMAC 與 Complete Binary Tree 儲存與處理資料完整性與子檔案區塊資料完整性問題，Complete Binary Tree 為一「二元樹」，結構上有著樹高等於 $\lfloor log_2 n \rfloor$+1 的優勢，其中 n 為葉節點個數；我們考慮將每一子檔案的 MAC 碼對應到 Complete Binary Tree 的葉節點，再由下往上(bottom up)建置一對應到該檔案的 MAC 碼樹，以此為基礎研發偵測錯誤子檔的技術使其處理過程與樹高成線性關係，本論文開發的軟體就能在 $O(log_2 n)$計算效能內完成錯誤子檔的偵測工作，其中 n 代表子檔案總個數。在資料量較大的檔案，因其子檔案數量多，本論文此研發技術的效能就會非常明顯。另外，在此應用層面我們設計出將 Complete Binary Tree 的架構有效率地建置在軟體系統中的方法。

3.5 資料復原 (Data Recovery)

資料儲存於雲端儲存系統後，資料擁有者理論上不再留有原始資料，然而經前述本論文發展的偵錯技術如果發現資料不正確後，如何復原是必須嚴肅面對的問題，否則資料擁有者損失仍舊存在。本論文研發設計之軟體在此議題上，首先在資料上傳到雲端儲存系統時，同步上傳到兩個(含)以上的不同雲端儲存服務供應上的系統中，如圖三，同步上傳到 google drive 與 Amazon S3，此設計概念啟發自磁碟機陣列(Disk RAID)[2]技術，而且本論文在此刻意地建議選擇不同的雲端儲存服務供應商的系統，而不建議使用者選用同一供應商的兩個帳號作儲存，目的是不同的雲端儲存服務供應商資料會同時都錯誤的機率相對較低以及同時產生對儲存資料之危安事件可能性也較低。雖然我們有這樣的設計理念，但就使用者操作我們研發的軟體，他只需選擇執行一次上傳功能即可，由程式本體完成此多重儲存的工作，當然在本論文研發之軟體初始建置在使用者手機的過程，使用者即須提供其在雲端儲存服務供應商之系統的帳號與通行碼，而後續的上傳或下載資料的工作就完全由本論文研發的軟體代勞。使用者欲自雲端儲存系統下載檔案時，本論文研究設計的軟體需有效率地自雲端儲存系統下載各子檔作完整性的驗證或偵錯的處理，必要時作資料復原工作，最終使用者將取得完整的原始檔案資料。

3.6 私密性技術的應用

資料擁有者欲上傳的檔案在本論文發展設計的軟體內切割成適當大小的子檔後加密再上傳到雲端儲存系統，加密後的資料在上傳或下載的過程私密性即獲得確保，該資料在雲端儲存系統中因已加密也可以防治偷窺的攻擊。不僅如此，因為資料已加密，有朝一日資料擁有者自雲端儲存系統刪除該檔案後，縱使因雲端儲存系統的各種檔案管理模式或備份機制使該應已刪除的資料殘存在實體雲端儲存系統中，但因資料本身都已加密，沒有資料擁有者的解密金鑰，非法偷窺者甚至雲端儲存系統管理人員仍舊無法一窺資料本體的內容。而這加密程序的運作是在資料擁有者的手機上運作本論文所發展軟體完成，非假手其他系統可信度高。另外，在此加密的程序的設計上，本論文開發的軟體加密機制是以 AES[3]採 XTS[4]模式進行。

3.7 金鑰管理

無論是資料完整性或私密性運用密碼技術來達成這些目標之同時，必然會加入一關鍵性的秘密金鑰，此秘密金鑰的儲存非常的重要，如果為第三者所取得密碼技術之保護措施形同虛設，若不慎遺失則加密的資料恐永難回復，完整性的驗證也無法執行，這些金鑰我們考慮除了將放置在手機作業系統安全的管控區外，金鑰本體我們也考慮納入資料隱藏技術[7]做適當的保護；另外，也考慮用機密分享技術(secret sharing)來處理，金鑰被遺失或破壞後，金鑰復原的的工作。

肆、實驗結果

就雲端儲存系統之應用，本研究成果除了提供使用者手機自行以 XTS-AES 加密機制，確保資料的機密性外，更運用到 GAE 和 EC2 兩個雲端計算系統，主要目的為將上傳的資料透過樹根比對與數位簽章的檢驗，有效率地確保手機在與雲端傳輸資料時，資料的完整性，最後使用 google cloud storage 與 amazon S3 兩個不同的雲端儲存系統實際驗證我們的方法，達到儲存與備份的效果。

為求測試結果客觀性，我們從網際網路上下載三個不同大小的政府公開文件做測試，測試資料的相關資訊，請參考表一。本研究測試使用的手機型號為 HTC One_M8，android 環境為 6.0 版本，CPU 運算速度為 2.5GHz，記憶體大小為 2GB，網路傳輸通道為中華電信光世代上傳 40M 下載 100M 方案。

表一：測試資料資訊

	檔案一	檔案二	檔案三
名稱	科技部秘書處科員職務應徵人員基本資料.docx	核定清冊 0207.xlsx	2018-2019 台匈(HAS)及台保(BAS)雙邊人員交流 PPP 計畫核定補助名單.pdf
大小	14.22KB	24.84KB	68.50KB
所在網址	https://www.most.gov.tw/most/attachments/a8271f44-8b60-4215-b0d9-eddc21da0bdc	https://www.most.gov.tw/nat/ch/detail?article_uid=2063898f-b66b-4f4c-a7a6-92886b213442&menu_id=d3c30297-bb63-44c5-ad30-38a65b203288&content_type=F&view_mode=gridView	https://www.most.gov.tw/most/attachments/5f2cb5ea-f6fc-43c4-9a7d-afdadc9604a1

本研究以 google cloud storage 和 amazon S3 兩個系統做為測試雲端儲存伺服器。表二為實驗測試結果；下載的測試中，我們設計下載檔案正確和檔案發生錯誤兩種情境，以瞭解發生錯誤後資料復原所需的時間，表二的結果可以明顯看出檔案有錯時，我們的方法只需原來下載時間一成左右的時間即可復原檔案，雖然此復原過程需自另一雲端儲存系統下載部分資料，而且此因應錯誤所耗費的時間隨著檔案越大，產生的效益比例越明顯。

表二：測試結果

網路上傳速度：29.951Mbps		網路下載速度：102.851Mbps	
	上傳時間	下載時間	檔案錯誤下載時間
檔案一	16129 毫秒	4089 毫秒	4816 毫秒
檔案二	27653 毫秒	7071 毫秒	7564 毫秒
檔案三	62451 毫秒	17011 毫秒	17945 毫秒

伍、結論

本研究完成之系統提供下列安全功能，資料上傳至雲端與下載過程資料私密性、資料上傳與下載過程資料完整性、儲存於雲端儲存系統資料私密性、儲存於雲端儲存系統

資料完整性、雲端儲存系統檔案儲存受到不當破壞的可歸責性、$O(log\ n)$內有效率的偵測錯誤檔案資料區塊與有效率的復原錯誤資料區塊。此外本研究開發之機制在資料擁有者與雲端儲存服務供應商間無需第三個系統支援，在下載檔案發生錯誤區塊時，子檔案區塊總數為 n 因樹狀結構只需$O(log\ n)$搜尋時間，本研究成果大幅減少尋找錯誤子檔案的時間。但當檔案異動增刪幅度過於龐大時，會影響本研究設計的樹狀結構特性，因此未來研究工作為設計檔案上傳後，若因各項處理應用有大量的增刪檔案內容時，如何持續維護樹狀結構之 complete binary tree 特性，才能維持本論文技術因應發生錯誤資料可以降低時間成本的功效。

參考文獻

[1] M. Bellare, R. Canetti and H. Krawczyk, "Keying Hash Functions for Message Authentication," *Annual International Cryptology Conference*, pp. 1-15, Springer, 1996.

[2] P. M. Chen, E. K. Lee, G. A. Gibson, R. H. Katz and D. A. Patterson, "RAID: High-Performance, Reliable Secondary Storage," ACM Computing Surveys (CSUR) vol. 26, pp. 145-185, ACM, Jun. 1994.

[3] J. Daemen and V. Rijmen, *The Design of Rijndael: AES – The Advanced Encryption Standard*, Springer-Verlag, Nov. 2001.

[4] M. J. Dworkin, "Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices," *NIST Special Publication 800-38E*, National Institute of Standards and Technology, Jan. 2010.

[5] *IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices*, IEEE Xplore Digital Library, Apr. 18, 2008. doi:10.1109/IEEESTD.2008.4493450. ISBN978-0-7381-5363-6.

[6] K. Jamsa, *Cloud Computing, SaaS, PaaS, Iaas, Virtualization, Business Models, Mobile, Security and More*.

[7] M. Raggo and C. Hosmer, *DATA HIDING Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols*, Elsevier, Nov. 2012.

[8] W. Stallings, *Cryptography and Network Security Principles and Practice seventh Edition*, 2017.

[9] 林華鵬、周國森、郭志勇、單張麟、陳彥仲、林宗毅，"雲端安全儲存系統"，*TANET2013 台灣網際網路研討會[論文集]*。