智慧型裝置應用於雲端資料共享之安全防護研究

陳信北、陳維魁、邱業桐
健行科技大學資訊工程系
hpchen@uch.edu.tw、wkchen@uch.edu.tw

摘要

近年來雲端運算技術的發展較著重於基礎的建設與服務的提供，在資訊安全方面只有簡單的網路控管與簡易帳號識別等。本研究的內容主要針對雲端資料共享安全之身分識別與存取管理方面進行研究。本研究將改良目前現有廣泛流行的一次性密碼系統(One-Time Password; OTP)技術為互動式行動 OTP(Interaction Mobile OTP; IMOTP)於智慧型行動裝置上與 PKI(Public Key Infrastructure)系統相互結合，應用於雲端硬碟之資料共享安全的機制上。我們將利用系統每回隨機產生的視覺碼(Vision-Code)做為交互詢答認證的基礎，由行動裝置 APP 應用程式運算完成後得到 IMOTP 互動安全碼，去登入身分認證識別，並利用 PKI 系統對共享資料做加密。此系統將與現行雲端硬碟登入方式(如；帳號密碼認證、OTP 登入認證)做比較，進行各項網路攻擊之竊取行為模擬並做安全分析。相信系統模擬結果可提高雲端硬碟資料共享的安全性。

關鍵詞：一次性密碼系統、IMOTP、資料共享安全、互動安全碼

壹、前言

雲端運算(cloud computing)[1]-[3]可提高應用程式部署速度、促進創新和降低成本，同時增強企業經營的敏捷性。隨著雲端服務應用的擴展，雲端運算的安全問題也將逐漸顯現[5]-[9]。而導致這些隱患的，並不是由於技術本身，或者故障發生，而是由於資訊安全控管等人為的錯誤，造成所有人都能看到數以千計客戶的私人資訊的問題。在電腦世界越來越導向「雲端運算」之際，保護個人資料更有其必要，因為「雲端運算」意謂在網路上共享的伺服器上儲存資料。網路設備業者 Juniper 表示，雲端運算及行動裝置上的安全問題更應該受到重視，隨著行動裝置的普及，行動辦公室等靈活的工作模式相繼興起，企業對網路的效能及安全水準的要求將愈來愈高。

近年來雲端運算技術的發展較著重於基礎的建設與服務的提供，在資訊安全方面只有簡單的網路控管與簡易帳號識別等[10][11]。然而，服務的提供卻得不到使用者對資訊安全的信任，造成目前大都不放心將機密性或敏感性資料儲存於公用雲端上。因此，本研究主要針對雲端運算的資訊安全問題為探討的目標。內容主要針對身分識別及存取控制管理(Identity and Access Management; IAM)方面。對於企業應用而言，現今 IT 部門面臨的最大的挑戰之一就是身分和存取控制管理。當企業也許有能力調控數個雲端運算服

務，但沒有好的身分和存取控制管理策略，終將造成嚴重資安事件。因此，對線上使用者而言，身分和存取控制管理策略是第一個要考慮的資安問題。

隨著網際網路越來越普及化，逐漸改變了人們的生活型態，而身分識別是網路服務最基本的建設，例如電子商務、政府電子化及 Web 服務的發展漸趨成熟，伴隨著資訊安全風險也增加，因此，身分識別為一重要的課題。傳統身分識別提供使用者一組固定的帳號與密碼。近年來電腦病毒、木馬程式、電腦蠕蟲、釣魚網站、間諜程式、暴力破解等不法技術的進步，密碼儘管使用 SSL 加密協定，也變得不再安全。一旦帳號/密碼遭有心人士竊取，使用者身份可能因此被冒用，輕者造成個人財物損失，重者公司機密資料外洩等，無法彌補的損害。為了防止帳號/密碼被竊取，目前已發展出一次性密碼機制(One-Time Password; OTP)，利用密碼產生器依據演算法運算，具有不可預測、不可重複、使用一次或時間過即失效等特性。

然而一次性密碼的機制面對釣魚網站[4]的攻擊手法是有風險的，釣魚網站利用社交工程的方式寄送假造的電子郵件，誘騙使用者連結至相似度高偽造的網頁介面，竊取使用者所登入的帳號/密碼。由於被竊取的密碼並未於真正的合法介面上登入過，且一次性密碼於一定期間內為有效的密碼，因此，有心人士於有效期間內利用被竊取的密碼登入真正的合法介面即可冒用使用者的身份。綜上所述，如何做到互動雙向保護認證讓使用者可於認證過程中分辨出偽造的服務界面，於帳務性交易或機密性資料查詢系統時得到更多的防護，提高安全性，有效的保護措施便是目前極需努力的目標。

雲端運算聯盟提出資料的生命週期[12]，把資料的過程是區分為創建(Create)、儲存(Store)、使用與共享(Use and share)、歸檔(Archive)、銷毀(Destruct)等階段，其中使用與共享是雲端運算上資料生命週期重要的一環。越來越多的使用者與企業利用雲端硬碟來儲存與共享資料。因為可以提高作業程序的便利性，減少不必要的來回運送時間與費用，也方便資料整合，因此，個人與企業使用情況愈來愈多。在雲端運算環境中，資料可從一個地方移動到其他地方，除了儲存雲端中，資料也可能頻繁移動到客戶端並且通過不安全的網路傳輸，導致資料安全上的威脅，如何做到雲端上資料保護值得我們探討的問題。

首先我們可以看到不管是 Google 雲端硬碟[13]、Dropbox[14]、Microsoft SkyDrive [15]，大多數雲端硬碟提供商都是使用帳號密碼來做身分認證登入方式，這種方式很容易讓駭客或有心人士利用簡易的攻擊手法竊取其帳號、密碼，進而登入該使用者的雲端硬碟導致個人或企業重要資料外洩，造成無法彌補的損害。圖一為 Google 雲端硬碟網頁登入頁面，圖二為 Dropbox 的網頁登入頁面，圖三為 Microsoft SkyDrive 網頁登入頁面，皆使用簡單帳號、密碼登入認證方式。

再來看到，不管是 Google 雲端硬碟、Dropbox 除了提供儲存檔案的平台外，也都具備資料夾共享的功能，讓使用者可以將特定資料分享給多人存取，且一個資料夾裡可以包含許多檔案，並讓其他共享者同步更新同一個資料夾，達到即時分享資料檔案的目的。

然而這些資料分享大多是只使用電子郵件或者使用者名稱來提供資料分享連結，這樣的方式可能因疏忽輸入錯誤電子郵件者，導致資料分享錯誤的人。

圖一：Google 雲端硬碟登入頁面

圖二、Dropbox 登入頁面

圖三、Microsoft SkyDrive 網頁登入頁面

圖四為 Google 雲端硬碟資料分享頁面，圖五為 Dropbox 的資料分享頁面，如下所示，皆使用電子郵件方式共享文件機制。針對雲端運算環境資料共享之安全研究有：Kao Yung-Wei 團隊於 2013 年發表 IET 期刊論文[16]主要使用 QR-code 做為雲端身分認證方式，並使用加密處理資料。國外已發表針對雲端運算環境資料共享之研究有：新加坡 I2R 的 Cheng-Kang Chu 團隊於 2013 年 10 月於 IEEE Pervasive Computing 期刊發表一篇[17]論文，主要針對目前三大雲端共享之缺點，提出安全共享連結 URL，並未針對身分認證與資料加密提出研究。S. Sundareswaran 團隊於 2012 年 IEEE Transactions 期刊上發表[18]論文，主要使用 ARJ 的自動登入認證機制為資料共享認證，並提供分散稽核追蹤機制。Junbeom Hur 於 2013 年於 IEEE Transactions 期刊上發表[19]論文，建議了一個 CP-ABE 方案，由建立存取樹開始，並產生金鑰執行加解密資料，及金鑰保管等研究。Xuefeng Liu 團隊於 2013 年於 IEEE Transactions 期刊發表 [20]論文，提出一個 Mona 的方案，主要包含系統初始化、使用者註冊、使用者撤銷、共享檔案建立、刪除、存取追蹤等程序。Larry A. Dunning 於 2013 年於 IEEE Transactions 期刊發表[21]論文主要提出資料共享時通訊負擔(overload)的改善機制。

圖四、Google 雲端硬碟資料分享頁面

圖五、Dropbox 的資料分享頁面

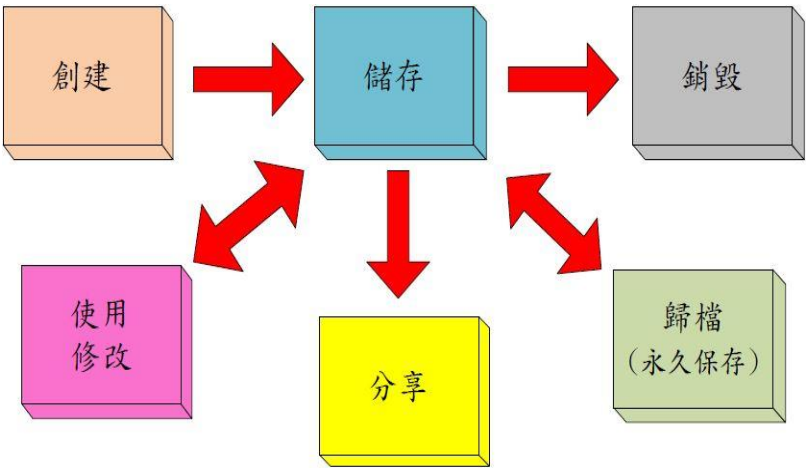
本研究將資料生命週期過程中的資料使用共享(Share)階段安全改善為主要目標。資料使用共享是現今在雲端硬碟中被大規模的建置與應用。我們提出可行的雲端資料共享加密系統方案來改善此階段的安全性問題。改良目前現在廣泛流行的一次性密碼(One-Time-Password; OTP)技術為互動式行動 IMOTP(Interaction Mobile OTP; IMOTP)來加強在雲端身分驗證機制上的安全。並採用資料分級來達到資料擁有者免於開放權限給

不是在該共享資料群組的人，讓跨權限的存取資料的問題疑慮降至最低，並將資料分類為最高權限安全需求的情況下使用 PKI 之加密技術來達到雙重安全的資料保護，並確保共享使用者如被駭客攻擊，資料遭竊取也無法馬上解讀資料內容來確保其機密性。藉此讓機密性資料或一般性資料都可以有彈性去選擇資料權限等級，讓使用者達到想要的安全性，並減少使用者在資料共享使用上的安全疑慮，提高服務之安全性。

貳、先前技術探討

首先介紹 MOTP(Mobile One-Time Password)行動動態密碼系統、其次介紹資料生命週期階段與各階段威脅分析。行動動態密碼系統(Mobile One-Time Password；MOTP)簡單來說就是行動裝置 OTP，就是裡用行動裝置來當作 OTP 使用者的媒介，取代傳統 OTP Token 來做 OTP 密碼的產生器，在使用者依據自己手邊的行動裝置選擇自己常用的行動裝置並將 OTP 安裝於行動裝置上，來做身分認證之用。MTOP 採取的是軟體安裝的方式因此可以將數個 OTP 程式安裝在同一個行動裝置上，對比傳統 OTP 來說，如果 OTP 系統更換就需要重新更新 OTP Token ，當使用多的 OTP 系統時，就不需要使用多個 OTP Token，集中管理安裝於同一個行動裝置是相當方便。MTOP 軟體如同一般應用程式，所以才會強烈建議安裝在個人行動裝置上來達到高安全性，假如安裝在 PC 或 NB 上有可能中了木馬程式後駭客也可以取得 OTP Token 的使用權 所以才需要建議安裝於手機或平板上盡量使用合法軟體來確保 OTP Token 安全性。

資料的生命週期模型，在甲骨文(Oracle)白皮書[22]中提到資料生命週期存取頻率，隨著時間的推移資料的存取將逐漸變少，最後會將資料移動到資料庫歸檔(永久保存)的狀態，整個生命週期包括三個狀態：活躍狀態(active state)，低活躍狀態(less active)，歷史狀態(historical state)或封存狀態(archived state)。在雲端安全聯盟中[23]，提出了資料安全性，生命週期的概念歸納成六個流程的資料生命週期包含：創建、儲存、使用修改、分享、歸檔(永久保存)和銷毀。基於上面敘述的定義，我們建議生命週期的模型圖如下圖六所示。



圖六、資料生命週期模型

資料安全性非常重要，儘管雲端運算服務的優勢在資料儲存，但安全問題使人們猶豫不敢嘗試雲端資料儲存服務，無論是雲端服務提供商還是雲端使用者，都希望雲端運算環境有足夠的安全性。因此，將資料生命週期使用共享與修改儲存可能發生的資料安全威脅問題做了簡要敘述：

- 資料傳輸：當使用者在儲存資料的過程中使用不安全的網路環境，導致資料在傳輸過程中遭有心人士竊取。
- 資料儲存：做為資料第三方雲端服務，最大威脅就是訊息洩漏，資料需不需要加密儲存在雲端中降低訊息洩漏的風險。
- 資料的有效性保護：在雲端環境中，資料可能儲存在不同的設備上，如果某些設備或節點失效，可能導致資料無法使用，所以雲端運算應確保有效性的品質。
- 資料的備份和復原機制：當資料遇到天災或人禍時資料的備份或存放地點都有很重要的因素，所以該存放的距離跟保護資料的地方都需要被考量。
- 金鑰管理：資料的移動儲存加密過程中會有許多的金鑰，因此金鑰管理也決定了資料的安全性。金鑰管理相關的問題包括金鑰的生成，發佈，儲存，使用和銷毀。金鑰管理在資料保護的問題中也是複雜的一項。
- 資料一致性保護：使用者要使用的資料是需要保持在最新狀態，資料的一致性在共享模式下是很困難的，因為要確保使用者的先後使用次序跟儲存方式，所以資料的讀寫權限該怎麼定義也是一項問題。
- 資料完整性保護機制和完整性驗證：資料的完整性保護機制是確保資料再儲存前是正確的，資料完整性驗證是雲端運算服務檢查資料是否擁有者的資料正確無誤在雲端中，這兩個要求避免造成資料遺失或損毀。
- 權限管理：資料在雲端中大家都有不同的權限跟不同的存取資料的用戶，因此權限的管理包括許多問題，例如權限的定義，權限的分配，權限的更新，取消等等。

- 遠端平台認證：一個不可靠的雲端運算平台對資料安全是極大的威脅，所以該怎麼確保平台的認證安全也是問題。
- 身分認證：身分認證的目的是防止未經授權的用戶存取資料的問題。
- 存取控制：無論是儲存還是雲端運算平台都需要存取檢查，存取控制可以阻止雲端運算環境中外部的入侵攻擊等問題。

參、雲端資料共享安全機制

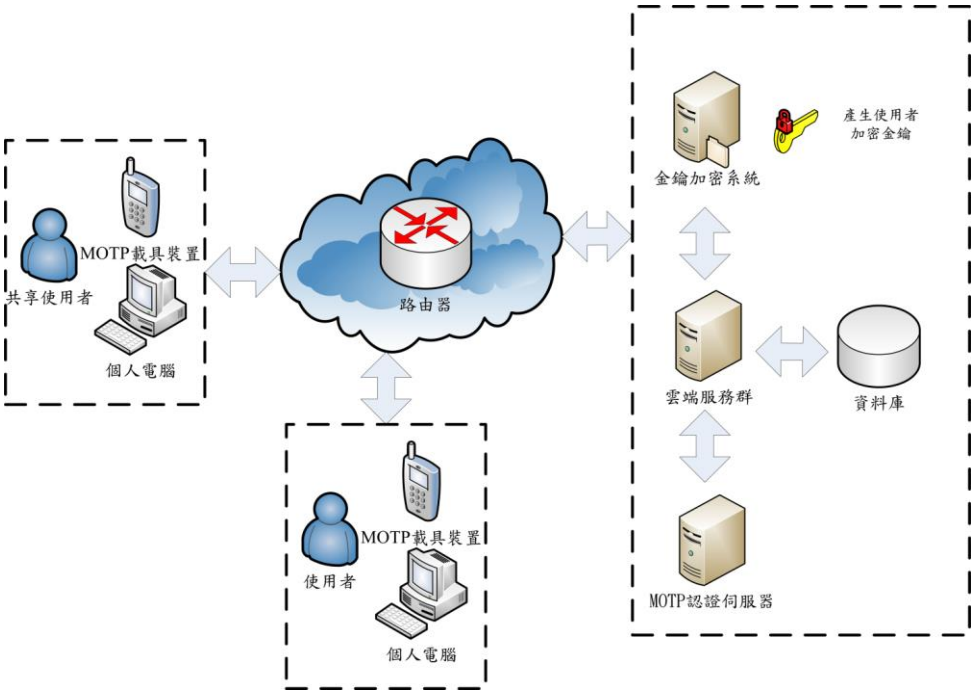
此節介紹本研究提出之雲端資料共享加密分級系統(以下簡稱本系統)，本系統將有別於現今雲端硬碟只有使用傳統的電子郵件帳號與密碼來登入與資料在分享的做法，在此階段上我們將增加資料的安全的保護與措施，以下各小節內容將分別介紹本系統的架構圖、註冊程序、使用者與分享使用者流程演算法等。

3.1 雲端資料共享加密分級系統架構

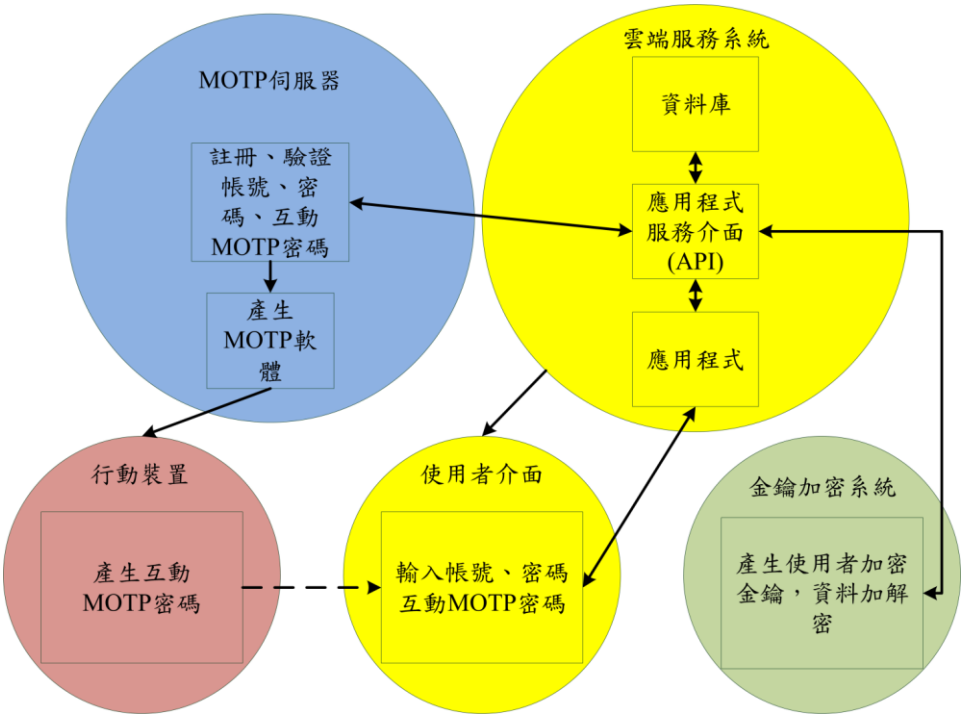
圖七為雲端資料共享加密分級系統架構圖。從架構中可以了解，使用者在前端使用自有行動裝置，而且裝置必須已經向 MOTP 伺服器認證和註冊雲端使用者，當使用者有需要把資料分享而資料權限在高安全性時，使用者資料就會藉由雲端服務群將資料庫中資料透過金鑰加密系統來做資料加密，進而透過協作平台來分享給使用者指定的人員來使用共享，當分享使用者要使用時在透過身分認證後，利用密鑰來解密資料完成資料讀取。

本系統架構主要區分五大部分，如圖八為雲端資料共享加密分級系統功能區塊圖所示。分別各區塊功能分別說明如下：

- 行動裝置：此為使用者行動裝置，但必須向 MOTP 認證伺服器做註冊。行動裝置註冊時 MOTP 認證伺服器將會指派一組裝置初始金鑰值給此裝置。註冊後行動裝置安裝 MOTP 安全認證碼程式並認證此裝置，行動裝置主要可取得運算後產生的一組互動 MOTP 安全碼並作為一種認證。
- 使用者介面：此為使用者登入應用程式視窗介面，主要為雲端硬碟登入帳號密碼與 MOTP 安全密碼輸入介面及視覺碼的顯示產生。當使用者連線至登入畫面時，把視覺碼輸入行動裝置上，運算後的 MOTP 安全碼在限制時間內，同時輸入使用者帳號、密碼、MOTP 安全碼等值，並傳送回 MTOP 認證伺服器驗證。



圖七：雲端資料共享加密分級系統架構圖。



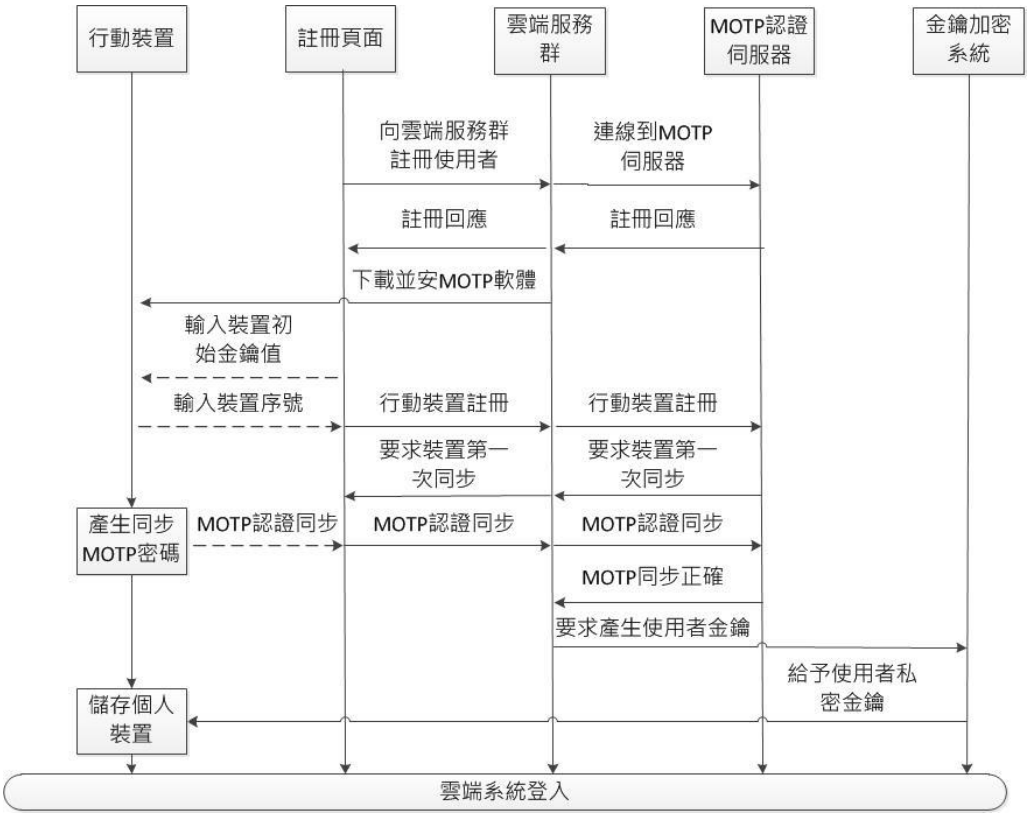
圖八：雲端資料共享加密分級系統功能區塊圖

- 雲端服務系統:此為主要雲端應用程式與大量資料儲存所在,其中包含了呼叫 MOTP 認證伺服器的應用程式服務介面，金鑰加密系統溝通與雲端應用服務，使用者與分享使用者資料管理，資料分享分級與應用程序、資料存取使用等。
- 金鑰加密系統：此系統為提供使用者非對稱式金鑰對。此金鑰對有兩個用途。一是對資料庫系統資料做永久性加密並儲存於資料庫中。使用者讀取資料後於自身裝置利用私密金鑰解密並存取應用。另一為，資料共享使用，利用被分享者非對稱式之公開金鑰將分享資料做一次性加密處理。當使用者分享資料時雲端服務系統將會從資料庫把要共享之資料移交由金鑰加密系統來判讀作解密，再做一次性加密處理，並移交回雲端服務系統。然後再將資料傳至被分享使用者，被分享使用者身分認證無誤後，使用自身私密金鑰解密資料，同時可直接讀取或是修改。
- MOTP 伺服器:此為 MOTP 認證伺服器，包含註冊、產生 MOTP 客戶端軟體、驗證帳號、密碼、互動式 MOTP 安全碼產生與驗證。主要工作是使用者與分享使用者存取要求中、高安全權限資料時的認證，並且需透過雲端服務系統的應用程式服務介面 API 來呼叫 MOTP 認證伺服器執行，以提高其安全性。

3.2 雲端資料共享加密分級系統註冊程序

使用者自有行動裝置需進行註冊。圖九所示為簡化之雲端資料共享加密分級系統註冊流程。說明如下：

1. 使用者於註冊頁面向雲端服務系統提出申請註冊使用者。
2. 使用者依據頁面說明新增註冊使用者個人相關訊息資料後送出至雲端服務系統。
3. 雲端服務群呼叫 MOTP 認證伺服器並依據註冊使用者之電子郵件地址發送軟體程式下載位置通知給註冊使用者。
4. 使用者依據下載點下載 MOTP 客戶端軟體，並安裝到 MOTP 行動載具裝置上，在此為個人行動裝置，如手機、平板電腦一類。
5. 使用者輸入 MOTP 認證伺服器給予之初始金鑰值至行動載具裝置上。
6. MOTP 行動載具裝置會產生一組”裝置序號”，使用者需於註冊頁面輸入，並回傳至 MOTP 認證伺服器。
7. 行動載具裝置產生第一組 MOTP 安全密碼，使用者於註冊頁面將密碼輸入，並回傳至 MOTP 認證伺服器同步驗證。
8. 同步驗證成功後，雲端服務群要求金鑰加密系統產稱使用者金鑰。
9. 雲端系統並給予註冊者一組非對稱式金鑰之私密金鑰到客戶端儲存裝置上。
10. 使用者進入登入介面，利用行動載具裝置產生 MOTP 安全密碼。並於登入頁面輸入帳號、密碼與 MOTP 安全密碼，傳送後端進行驗證。驗證成功後登入雲端服務系統。



圖九、雲端資料共享加密分級系統註冊流程圖

3.3 雲端硬碟資料分級機制

雲端硬碟在發展的過程中各家都有自己的資料共享方式與方法，然而鮮少有針對資料安全性等級為基礎去考慮資料共享的安全機制，本研究以資料安全性等級區分為公開性資料、低安全性資料、中安全性資料、高安全性資料四級，分別說明如下:

- 公開性資料:在公開性資料層級的資料通常是讓使用者們可以直接共享與公開的資料，在這個區域的共享機制下的使用者只須要透過超連結的方式就可以使用或者瀏覽此資料不必經過太多安全手續就可以直接存取，擁有者都可直接於雲端隨身碟上傳、下載與分享給其他人使用。例如廣告信件、宣傳品等。
- 低安全性資料:在低安全性資料層級的資料通常都是使用者認為不須特別安全保護的資料共享區域，在這個區域的共享機制下分享使用者只須要用簡單的帳號、密碼登入驗證直接進入到雲端硬碟協作平台來使用資料，低安全性資料的種類，例如:組織企業內部公開之資料、音樂、圖片、影片、文件、應用程式等，資料擁有者認為這些資料就算被駭客竊取也不會有較大損害，此類的資料都屬於低安全性資料。
- 中安全性資料:在中安全性資料層級的資料防護比低安全性資料多了一道程序，在分享使用者端將提高身分認證規格來達到資料分享的安全性，使指定的分享使用者才能

進入雲端硬碟協作平台來存取資料,所以在這層級的分享使用者們都需要在登入時輸入帳號、密碼及 MOTP 安全碼這三項來達到認證。中安全性資料的種類，例如:私人文件、資料、音樂、影片、圖片、應用程式等，在這層級資料擁有者需要中等安全保護，被分享人員要經過身分認證後才能存取，如資料外洩可能造成個人損害，此屬於中安全性資料。

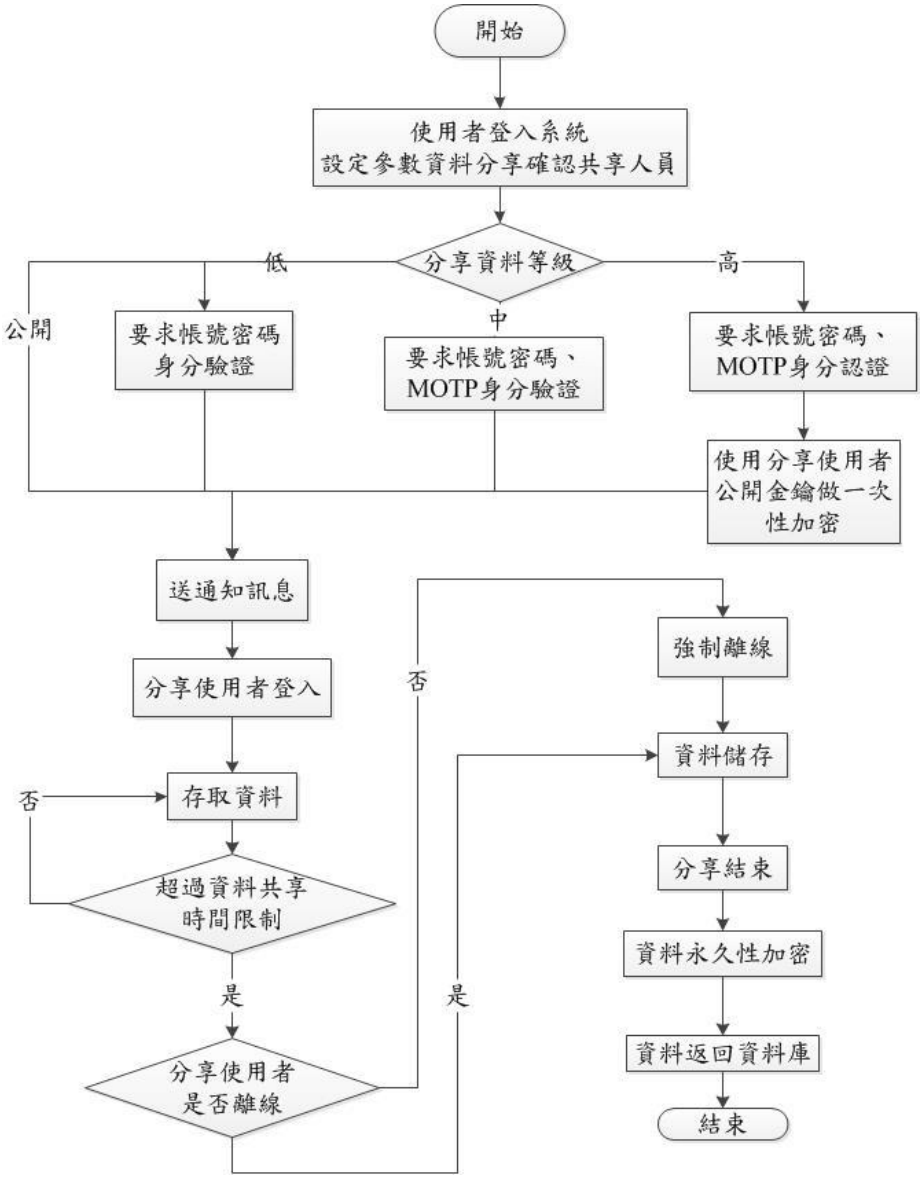
- 高安全性資料:在高安全性資料層級的資料防護比中安全性資料再多一道安全程序，在此的共享資料文件都會經過金鑰加密系統做資料一次性加密動作,此動作是取指定的分享使用者於系統之公開金鑰對共享資料做一次加密。因此，指定的分享使用者進入雲端硬碟協作平台來存取資料時，同中安全性資料防護機制，都需於登入時輸入帳號、密碼、MOTP 安全碼這三項來達到第一步身分認證。分享使用者點選共享的資料時就會發現資料是被加密的文件,此時需要透過系統分配之私密金鑰把資料作解密動作還原資料。高安全性資料的種類，例如:公司企業或組織機密文件等資料，需要被高度保護的資料類型都應選用此機制。

3.4 使用者資料共享程序與共享使用者資料存取程序流程

資料共享必然有原擁有使用者與共享使用者兩個不同的角色，而在資料分享過程中，兩方處理的程序大不相同，因此，本節將說明使用者資料共享程序與共享使用者資料存取程序流程，分別說明如下：

1. 使用者資料共享程序:使用者首先須確認要共享資料內容並依需求設定資料安全等級與共享人員，並通知共享人員。資料等級分成公開性、低安全性、中安全性、高安全性來做判斷。其中低安全性只需驗證帳號密碼，中安全性驗證帳號密碼、MOTP 安全碼三項。高安全性資料在共享前會先執行資料加密動作，將分享使用者在系統的公開金鑰，對共享資料做資料加密。當分享使用者登入，分享使用者會被通知該資料需使用自有的私密金鑰來做資料解密。通過驗證後接者存取資料，當所有分享使用者都存取結束或超過設定分享時間 Tout 時，使用者將共享資料功能結束，資料返回資料庫並做加密儲存，結束流程。使用者資料共享程序流程圖，如圖十所示。
2. 共享使用者資料存取程序流程：共享使用者接收到使用者的分享通知，連線到雲端服務群。如果為公開性資料，可直接讀取。如果為低安全性資料，就會連結到系統登入頁面要求輸入帳號密碼。如果為中安全性資料,除了要求輸入帳號密碼外,還需 MOTP 安全密碼驗證後才能登入系統存取資料。如果驗證錯誤 N 次以上系統會鎖定帳號並通知使用者及停止分享流程。如果為高安全性資料,除了要執行中安全性資料共享防護機制外，系統會提示為高安全性資料需要利用自有的私密金鑰執行解密資料。通過上述驗證防護機制後才可以開始存取資料並在修改過程中隨機儲存。系統會檢核是否

共享時間超過設定共享限制時間 Tout，如是直接強制所有共享人員離線並結束流程。共享使用者資料存取程序流程如圖十一所示。

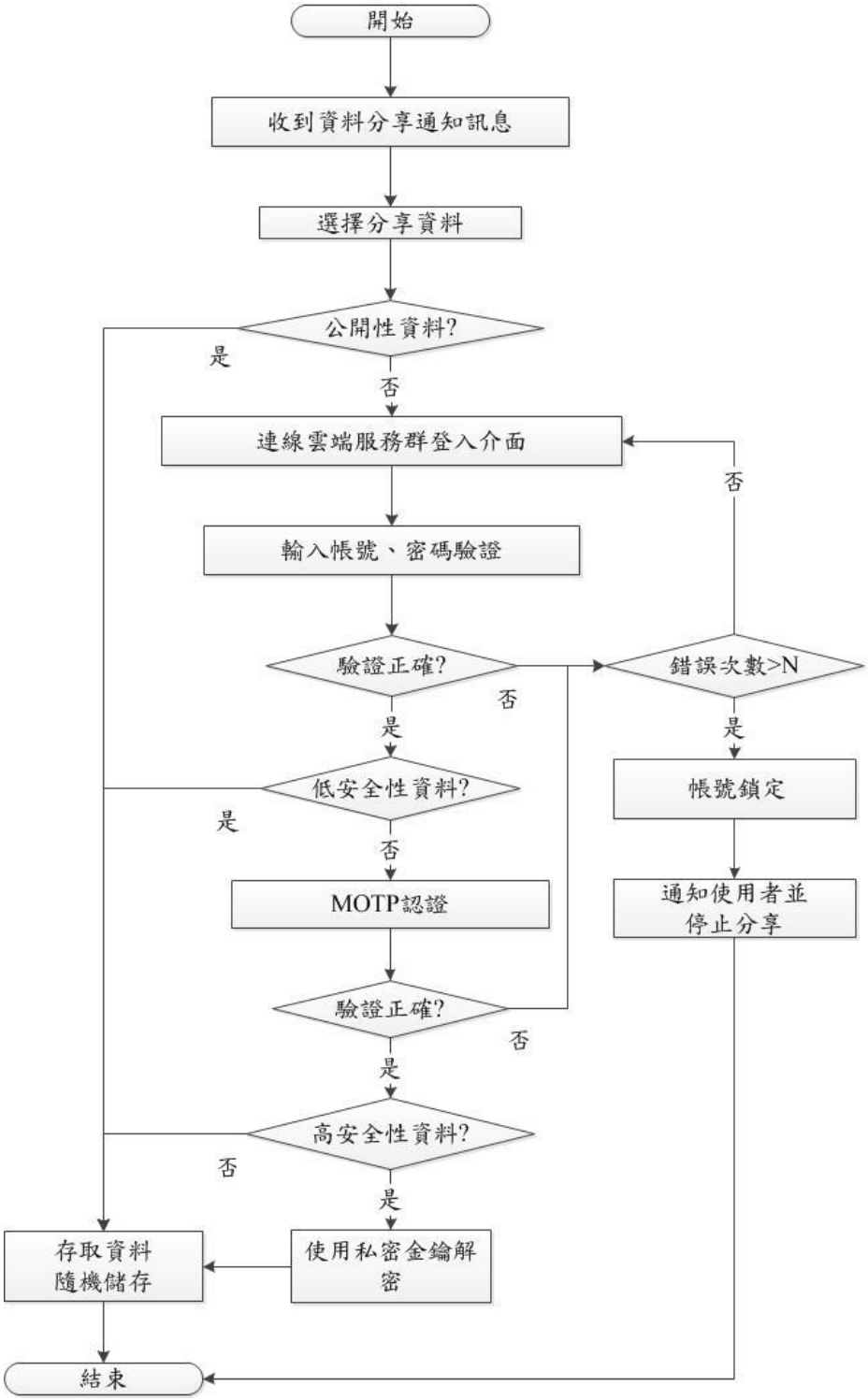


圖十：使用者資料共享程序流程圖

肆、實驗模擬與安全分析

在本論文中我們將模擬雲端運算資料共享方式並做比較，再依目前常見的幾種網際網路攻擊手法做安全性的分析，如暴力攻擊(Brute force attack)、鍵盤側錄攻擊(Keystroke logging)、重送攻擊(Replayed Attack)、中間人攻擊(Man-in-the-middle attack)、字典攻擊

(Dictionary attack)等。



圖十一：共享使用者資料存取程序流程圖

4.1 雲端資料加密分級系統運作

使用者在開始分享資料並確定分享使用者人員，儲存後系統將自動發送通知訊息到分享使用者的行動裝置上告知分享使用者可以連線到雲端服務群做登入存取，分享使用者進入服務系統之第一道防線就是帳號、密碼、MOTP 互動密碼登入介面，MOTP 伺服器會隨機發送一組 MOTP 視覺碼，並傳送到登入畫面上及限制時間 Tout，如下圖十二為分享使用者接收到通知訊息、圖十三為雲端服務群登入畫面。

圖十二：分享使用者接收到通知訊息

圖十三：雲端服務群登入畫面

分享使用者開啟行動裝置 MOTP 載具的 MOTP 互動式密碼系統軟體，輸入登入頁面上的 MOTP 視覺碼，行動裝置 MOTP 載具產生 MOTP 安全碼，並將 MOTP 安全碼傳送回 MOTP 伺服器驗證，必須在有效時間內進行驗證，如果超過有效時間內，須重新登入頁面方可重新產生 MOTP 視覺碼在執行驗證。如圖十四為產生互動式 MOTP 密碼。

圖十四：產生互動式 MOTP 密碼

將產生的互動式 MOTP 密碼與帳號、密碼輸入於登入頁面，系統將分享使用者資訊

與互動式 MOTP 密碼傳回 MOTP 伺服器端並進行驗證，驗證成功登入雲端共享服務，驗證失敗則顯示錯誤訊息，錯誤大於 N 次後則該帳號鎖定。圖十五為分享使用者登入帳號密碼 MOTP 密碼。當使用者成功登入雲端服務系統，系統服務區並共用設定可以分為公開、低、中、高安全性資料，在點選設定為公開性共享資料，只需要共享連結就可以使用資料；低安全性共享資料只需要簡單的帳號密碼認證就可以使用資料；中安全性共享資料裡面的資料會需要驗證電子郵件帳號密碼、互動式 MOTP 密碼後才能存取資料；高安全性共享資料，需驗證電子郵件帳號密碼、互動式 MOTP 密碼後，會跳出資料是有加密之視窗，在經過分享使用者利用私密金鑰來解密資料，解密完成才能存取資料。圖十六為雲端共享設定頁面。

圖十五：分享使用者登入帳號密碼 MOTP 密碼

圖十六：雲端共享服務頁面

4.2 安全性分析

本論文利用目前網際網路上常見的攻擊手法做安全性的分析，攻擊手法包含暴力攻擊(Brute force attack)、鍵盤側錄(Keystroke logging)、重送攻擊(Replayed Attack)、中間人攻擊(Man-in-the-middle attack)、網路釣魚(Web Phishing)。分別說明如下：

- 暴力攻擊：對於傳統的電子郵件、密碼登入方式，是可行的攻擊手法，原因在於暴力攻擊使用不斷的重複嘗試來針對密碼逐一進行測試破解，直到登入系統成功；在一般針對此類型的攻擊手段對策，設定一個強力的密碼原則，原則在於複雜化密碼、密碼長度、密碼最長使用時間、密碼錯誤鎖定。而資料共享加密分級系統，可有效防止暴力攻擊，其原因在於本系統具有不可預測、不可重複、使用一次或時間過及失效等特性並且將分享資料加密。在進入雲端服務區後當選取高安全性資料時就會被要求驗證電子郵件、密碼、互動式 MOTP 密碼，之後需要分享使用者的私鑰來進行解密動作。就算暴力破解獲取到使用者帳號密碼，然而在互動式 MOTP 密碼部分使用暴力攻擊登入，由於該分享使用者產生的互動式 MOTP 密碼每次都是不一樣的，當暴力攻擊進行三次後，會回傳密碼錯誤三次，則該分享使用者遭鎖定。

- 鍵盤側錄：可以記錄使用者在鍵盤上所打入的每個按鍵，再將資料傳送給駭客，由此可見傳統只用電子郵件帳號、密碼的方式，並非有效的防護能力。而在資料共享加密分級系統，可有效防止鍵盤側錄，其原因本系統具有動態密碼，每次登入時密碼都會有所改變。我們將鍵盤側錄程式安裝在分享使用者電腦上，當使用者要使用高等安全性資料時在鍵盤上輸入的每個按鍵，都會被鍵盤側錄程式所側錄到筆記本中，我們再將電子郵件帳號、密碼、互動式 MOTP 密碼再一次進行登入，結果失敗。因為互動式 MOTP 密碼具有一次性，每次使用者產生的都不一樣且具有時間限制，所以結果顯示密碼錯誤。
- 重送攻擊：將使用者的訊息於傳送中進行竊取，在將竊取的訊息重新傳送給認證伺服器，傳統的電子郵件帳號、密碼，只需將訊息進行重送即可登入系統，而在資料共享加密分級系統，可有效防止重送攻擊，在中、高安全性資料都有互動式 MOTP 密碼驗證，因此密碼登入過一次此 MOTP 密碼即失效，使用者隨機產生的互動式 MOTP 密碼也不可能與前一次相同，然而在高安全性資料時就算資料被竊取還有資料加密來做保護。我們將分享使用者登入互動式 MOTP 安全碼後進行封包重送，由於 MOTP 安全碼具有一次性的特性，進行重送攻擊時，MOTP 伺服器會回應 MOTP 密碼錯誤。
- 中間人攻擊：就是駭客偽造資料封包並在使用者與雲端伺服器中竊取，將竊取的資料修改再傳送給使用者，傳統的電子郵件帳號、密碼是無法防禦的，即使有資料傳送過程有 SSL 加密，駭客只需要一些時間來做解密，然而資料共享加密分級系統，可有效防止中間人攻擊，因為在於傳送過程中使用 SSL 加密有時間上的限制，駭客在短時間無法解密，並且資料也有做一次性加密的雙重保護。我們在使用者與伺服器之間進行封包擷取，傳送過程中使用 SSL 加密，並將擷取進行解碼，由於解碼過程須要花一段時間，在還沒完成解碼時，互動式 MOTP 密碼時效已過，無法再登入系統中。
- 網路釣魚：是偽造合法網站，利用誘騙使用者將登入資訊輸入非合法的網頁，並記錄下來，傳統的電子郵件帳號、密碼，將會被竊取，原因在於網路釣魚紀錄每個動作，然而資料共享加密分級系統，可有效防止網路釣魚，重點在於使用者讀取非法網頁中的視覺碼，此正常情況下視覺碼是由互動式 MOTP 伺服器產生，同時也有時間限制，當時間過後此視覺碼也就失效。我們製作一個釣魚網站，模擬使用者輸入電子郵件帳號、密碼、互動式 MOTP 密碼至釣魚網站，此時帳號密碼互動式 MOTP 密碼皆被側錄到釣魚網站的資料庫中，並顯示系統維護的假象給分享使用者螢幕上，我們在將所側錄到的結果輸入到正確的網頁中，由於互動式 MOTP 密碼具有時間上的限制，所以側錄到的資訊並無法解開高安全性資料，使用者端傳送互動式 MOTP 密碼錯誤的訊息。

  下表一為利用傳統電子郵件帳號密碼執行資料共享與資料共享加密分級系統對抵禦

各類型攻擊方式之比較。傳統電子郵件帳號密碼對於各類型攻擊手法，是完全沒有防禦的能力，而在資料共享加密分級系統能有效防禦常見的攻擊手法，改善傳統上的問題，並而提高雲端資料安全性。

表一：雲端運算資料共享方式與攻擊手法比較分析

攻擊類型	電子郵件帳號、密碼	資料共享加密分級系統
暴力攻擊(Brute force attack)	×	◎
鍵盤側錄(Keystroke logging)	×	◎
重送攻擊(Replayed Attack)	×	◎
中間人攻擊(Man-in-the-middle attack)	×	◎
網路釣魚(Web Phishing)	×	◎

<×代表不可抵擋、◎代表可抵擋>

伍、結論

在雲端運算使用日益增加，使用者能方便使用網際網路支援之餘，資訊安全問題也備受人們重視。本研究所提出的雲端運算資料共享之安全防護研究，可以在雲端硬碟資料的保護上能更為安全周延，防止有心人士或駭客對機密資料的竊取。我們在資料共享上增加了彈性，讓資料有分級制度，可避免資料誤用的可能性。互動式 MOTP 密碼具有不可預測、不可重複、使用一次後失效等特性，就算在雲端資料不慎被竊取，資料本身也做了加密處理，不但解決傳統雲端硬碟沒有加密資料的威脅，也改善了資料在雲端硬碟上的安全性。雲端運算的攻擊手法層出不窮，使用者依舊要多層保護，在身分認證上，使用雙因素認證，雲端資料共享安全機制等，在使用機密性資料時更應使用多層認證與保護機制，才能有更高的安全性防護能力。雲端運算是未來的趨勢，在資料共享之資安問題顯得更為重要，在身分認證登入或者在資料分享上的保護結合資料共享之安全防護機制，相信可以杜絕有心人士的不法竊取，提高系統安全性，提高使用者對雲端運算的信心。

參考文獻

[1] Sun Microsystems Inc., *Introduction to Cloud Computing architecture White Paper*, 1st

Edition, June 2009

[2] A. Weiss, *Computing in the Clouds*, Net Worker, vol. 11(4), pp.16-25, Dec. 2007

[3] B. Hayes, "Cloud computing", *Communications of the ACM*, vol. 51, no. 7, pp. 9-11, July 2008

[4] Anti-Phishing Working Group, Inc. http://www.antiphishing.org, 2012.

[5] K. Hwang, S. Kulkareni, and Y. Hu, "Cloud Security with Virtualized Defense and Reputation-Based Trust Mangement," *IEEE International Conference on DASC '09*, pp.717 – 722, 12-14 Dec. 2009

[6] L.M. Kaufman, "Data Security in the World of Cloud Computing," *IEEE Security & Privacy*, vol. 7, no. 4, pp. 61 – 64, July 2009

[7] M. Yildiz, J. Abawajy, T. Ercan, and A. Bernoth, "A Layered Security Approach for Cloud Computing Infrastructure," *2009 10th International Symposium on ISPAN*, pp.763 – 767, 14-16 Dec. 2009

[8] M. Jensen, J. Schwenk, N. Gruschka, and L.L. Iacono, "On Technical Security Issues in Cloud Computing," *IEEE International Conference on Cloud Computing*, pp.109 - 116 21-25 Sept. 2009

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in Cloud Computing," *17th International Workshop on Quality of Service*, pp. 1 – 9, 13-15 July 2009

[10] X. Huang, T. Zhang, and Y. Hou, "ID Management among Clouds," *2009 First International Conference on Future Information Networks*, 2009.

[11] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," *CloudCom 2009 LNCS 5931*, pp. 157–166, 2009.

[12] X. Yu and Q. Wen , "A View about Cloud Data Security from Data Life Cycle", *Proc of CISE*, pp1-4,2010

[13] Google 雲端硬碟, https://www.google.com.tw/

[14] Dropbox, https://www.dropbox.com/

[15] Microsoft SkyDrive, https://login.live.com/login.srf?

[16] Y.-W. Kao, K.-Y. Huang, H.-Z. Gu, and S.-M. Yuan," uCloud: a user-centric key management scheme for cloud data protection", *IET Information Security*, vol. 7, no. 2, pp. 144-154, 2013

[17] C.-K. Chu, W.-T. Zhu, J. Han, J.K. Liu, , X. Jia, and J.Y. Zhou, "Security Concerns in Popular Cloud Storage Services," *IEEE Pervasive Computing*, vol. 12, no. 4, pp. 50-57, 2013

[18] S. Sundareswaran, A.C. Squicciarini, and D. E. Lin, "Distributed Accountability for

Data Sharing in the Cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp. 556-568, 2012

[19] Junbeom Hur," Improving Security and Efficiency in Attribute-Based Data Sharing," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 10, pp. 2271-2282, 2013

[20] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 6, pp. 1182-1191, 2013

[21] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W.J. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362-375, 2013

[22] Oracle White Paper, *Information Lifecycle Management for Business Data*, http://www.oracle.com/, June 2007.

[23] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*, Nov. 2011.

[作者簡介]

陳信北：國立台灣科技大學電機工程研究所計算機組博士。現為健行科技大學資訊工程系專任助理教授。專長於網路技術、行動通訊、資訊安全之身分認證管理、網路安全。

陳維魁：國立交通大學資訊工程研究所博士。現為健行科技大學資訊工程系專任教授。專長於密碼學、資訊安全管理、電子商務安全。

邱業桐：健行科技大學資訊工程研究所碩士。專長於網路安全、資訊安全之身分認證管理。