iCloud 雲端服務之安全設計探討

何煒華
東吳大學資訊管理系
副教授
e-mail：
whhe@csim.scu.edu.tw

楊世鴻
東吳大學資訊管理系
研究生
e-mail：
01756014@scu.edu.tw

摘要

隨著智慧手機的發展，行動裝置越來越普及。透過 CSA 雲端安全指引所規範的雲端服務威脅，將 iCloud 安全控制措施作歸納分類並探討其安全性。

關鍵詞：CSA 雲端安全指引、雲端服務、iCloud

Abstract

With the development of smart phones, mobile devices are increasingly popular. Through cloud service threats specified by the CSA cloud security guidelines, the security controls for iCloud are categorized, and the security of iCloud are investigated.

Keyword: CSA cloud security guidelines, cloud service, iCloud

1. 前言

本論文探討 iCloud 雲端服務使用者在使用雲端服務功能的安全性分類，特別是手持裝置的使用。本章共分四節，第 1.1 節為研究背景；第 1.2 節為研究動機；第 1.3 節為研究目的；第 1.4 節為重要名詞解釋。

1.1 研究背景

iOS(之前稱為 iPhone OS)為 Apple 公司發展的行動裝置作業系統，最早在 2007 年用於 iPhone 與 iPod Touch，之後擴及至其他 Apple 裝置，如 iPadApple TV。有別於微軟 Windows CE (Windows 手機)Google Android，Apple 並不授權允許將 iOS 安裝在非 Apple 的硬體上[1]。甚至，iOS 必須使用 Apple 所推出的 iTunes 軟體，管理所有音樂、照片、影片及檔案等。蘋果的智慧型手機與平板電腦等行動裝置的可攜性與便利性，已成為今日行動化辦公工作環境中不可或缺的隨身工具。

由於這些行動裝置大都十分輕巧，卻可提供許多功能，如收發電子郵件、儲存文件及瀏覽簡報等，不僅可遠端存取資料，甚至是能存取其他網路設備。蘋果的 iCloud 雲端服務相當程度地提高生產力與工作效率，但同時使用者與企業也將面對蘋果的 iCloud 雲端服務所帶來的資安威脅。據 IDC 的估計，可存取網際網路之行動裝置將於 2013 年突破十億。除了各路業者積極爭取商機外，駭客更是覬覦這塊大餅，欲從中獲取龐大不法利益[11]。行動裝置作業系統廠商應儘速修改及強化作業系統安全，讓全球未來能有安全的行動裝置使用空間。儘管大部分的行動裝置之持有與使用係歸私人所擁有，很少有多人共用一台行動裝置之情形，但這也未必表示行動裝置是可信任的。另外，部分使用者會進行行動裝置的越獄(Jailbreaking)這行為會繞過行動裝置內建的安全防護機制，而給了惡意軟體很好的機會。

1.2 研究動機

發生於 2014 年九月發生名知 iCloud 資安重大事件[26]。本次事件的受害者大量儲存在 iCloud 的個人照片被盜，甚至一些已經刪除的照片都被駭客盜取，蘋果 iCloud 的安全性備受質疑，了解一般使用者在使用 iCloud 雲端服務時，是否會注意到資安風險的相關問題，如曝露敏感性資料。由此研究結果，找出適當的方式可降低因 iCloud 雲端服務造成的資安事件發生機會。以前使用手機只會考慮到電話的隱私性是否會被竊聽。現在則需要多保護這些敏感性的資訊被未經授權存取使用。譬如：在 iOS 手機應用服務上，不管是通訊錄、照片、安裝的應用程式及手機裡儲存的資料，都可與 iCloud 雲端服務整合。透過簡單的同步動作，在更換手機時就能自動將原有資料及設定同步使用。但如此便利服務的背後，一般民眾使用者是否有注意到資安風險的相關問題或是敏感性資訊曝露的風險。

iCloud 雲端服務的各種資安風險來源與研擬防護措施時的應注意事項，包括使用不可信任的軟體與裝置、使用不可信任的內容、缺乏實體的資安控制措施、使用不可信任的網路、與其他系統互動及情境範例說明。在瞭解資安風險與注意事項之後，本論文會針對 iCloud 雲端服務的安全提出使用建議。為了滿足以上的

資安要求，iOS 的行動裝置需要多項資安保護措施，部分資安功能是裝置本身內建，部分是額外附加的控制措施，再搭配裡其他資安控管作為，一起建構 iCloud 雲端服務資安防護措施。

之前 Furnell, Bryant, & Phippen [7]研究討論過桌上型電腦使用著資安風險意識但是沒有針對過在行動裝置使用雲端服務使用者之資安風險意識做詳細研究，本篇文章會探討 iCloud 雲端服務的使用者資安風險意識做詳細的研究。另外之前 Mylonas et al.[9]討論過行動裝置一般的資安功能做研究，但沒有針對專屬於 iOS 作業系統資安功能做資安功能的研究，這部分也是本篇論文加強探討的部分。先前 Mylonas et al. [9]只有針對一般社會大眾使用者研究，沒有針對特定群組使用者作差別研究。還有 Ally & Gardiner [4]只有針對使用者手持裝置使用接收度做研究，但沒有針對行動裝置的雲端服務資安風險接收度做衡量。

1.3 研究目的

智慧型手機再也不是只是單純的電話，行動裝置上面存取使用者敏感性資料的機會與內容越來越多，但是使用者對於這部分資安認知並沒有相對的跟上。雲端服務也將成為大部分使用者儲存數位內容主要方式，與傳統的電腦使用環境也有很大的區別 透過 CSA 雲端安全指引所規範的雲端服務威脅，將 iCloud 安全控制措施作歸納分類並探討其安全性。

1.4 重要名詞解釋

iCloud

iCloud[22][27]是蘋果公司所提供的雲服務，可以存儲音樂、照片、App、聯繫人和日曆等，將它們無線推送到用戶的 iOS 設備和電腦上，而無需完全受限於傳統接線方式將 iOS 設備插入基座與電腦同步。2011 年 5 月 31 日蘋果公司官方首次宣稱有 iCloud 的產品。蘋果公司宣稱 iCloud 將會取代 MobileMe，iCloud 是基於原有的 MobileMe 功能全新改寫而成，提供了原有的郵件、iCal 行事歷和聯絡人同步功能。可以自任何一部 Mac 或 PC 登入 iCloud.com，以查看所有儲存在 iCloud Drive 中的文件。也可以使用 iCloud.com 存取多種功能，例如照片、尋找我的 iPhone、郵件、行事曆、聯絡資訊等。iCloud 會儲存使用者的聯絡資訊、行事曆、照片、文件和更多項目，並在其所有裝置間自動保持最新的資料。iCloud 也可供第三方 App 用來儲存和同步文件以及 App 資料的重要數值，視開發人員所定義而定。使用者透過 Apple ID 登入並選擇想要使用的服務來設定 iCloud。IT 管理者可透過設定描述檔來停用 iCloud 功能。該服務無法得知正在儲存的內容，並會以位元組集合的方式對所有檔案進行處理。

圖1 iphone手機iCloud設定畫面

iCloud Drive

iCloud Drive 會加入以帳號為基礎的密鑰來保護儲存在 iCloud 中的文件[16]。和現有 iCloud 服務一樣，它會將檔案內容分塊並進行加密，然後使用第三方的服務來儲存這些加密區塊。不過，檔案內容密鑰是由記錄密鑰所封裝，與 iCloud Drive 資料儲存在一起。而這些記錄密鑰則由使用者的 iCloud Drive 服務密鑰所保護，儲存在使用者的 iCloud 帳號中。使用者可以藉由與 iCloud 進行認證來取用其 iCloud 文件資料受保護的部分。

圖2 iCloud Drive設定畫面

iCloud 備份

iCloud 還會每天通過 Wi-Fi 備份資訊，包括裝置設定、App 資料、相機膠卷中的照片和影片，以及訊息 App 中的對話。透過 Internet 傳

送內容時，iCloud 會對其進行加密，以加密的格式儲存並使用安全代號進行認證，進而保護內容。只有當裝置處於鎖定狀態、連接到電源且可透過 Wi-Fi 連接 Internet 時，iCloud 備份才會進行。透過 iOS 中所使用的加密技術，系統經過精心設計，既可保護資料安全，又能兼顧增量、自發式的備份和還原動作。以下是 iCloud 備份的項目[13]：

(1)已購買的音樂、影片、電視節目、App 和書籍的相關資訊，但不包括已購買的內容本身
(2)相機膠卷中的照片和影片。
(3)聯絡資訊、行事曆事件、提醒事項和備忘錄
(4)裝置設定
(5)App 資料
(6)加入到 iBooks 但未購買的 PDF 和書籍
(7)通話紀錄
(8)主畫面和 App 佈局
(9)iMessage、文字簡訊 SMS 和 MMS 訊息
(10)鈴聲
(11)HomeKit 資料
(12)HealthKit 資料
(13)Visual Voicemail

圖3 iCloud開啟手機資料備份設定畫面

當檔案從鎖定裝置時無法取用的資料保護類別中製作時，其檔案專屬密鑰會使用 iCloud 備份 Keybag 中的類別密鑰進行加密。檔案會以其原始的加密狀態備份至 iCloud。在資料保護類別為無保護中的檔案會在傳輸期間進行加密。iCloud 備 Keybag 內含每個資料保護類別的非對稱密鑰，這些密鑰用於加密檔案專屬密鑰。有關備份 Keybag 和 iCloud 備份 Keybag 內容的更多資訊，請參閱加密與資料保護一節中的鑰匙圈資料保護。備份集是儲存於使用者的 iCloud 帳號中，由使用者的檔案拷貝和 iCloud 備份

Keybag 組成。iCloud 備份 Keybag 受到隨機密鑰的保護，其也會與備份集一起儲存。使用者的 iCloud 密碼不會用於加密，因此更改 iCloud 密碼不會使現有的備份資料失效。當使用者的鑰匙圈資料庫備份至 iCloud 時，它仍會受到與 UID 連結的密鑰保護。這樣可讓鑰圈只能回復至原先產生它的同一台裝置，這意味著任何人都無法讀取使用者的鑰匙圈項目。回復後，備份的檔案、iCloud 備份 Keybag 和 Keybag 的密鑰將會從使用者的 iCloud 帳號取回。iCloud 備份 Keybag 使用其密鑰進行解密，然後 Keybag 中的檔案專屬密鑰則用於解密備份集中的檔案，這些檔案會被作為新檔案寫入到檔案系統中，進而根據其資料保護類別對其重新加密。

Touch ID

iPhone 的指紋辨識感應器 Touch ID，整合在 Home 鍵中，大小為 8x8 毫米，厚度 1 微米，以 500ppi 的解析度，讀取指紋的極細部特徵。它採用電容式觸控技術進行分析，將指紋歸類為三種基本圖案－弓紋、箕紋或渦紋，辨識出指紋的細部特徵，來進行比對。當使用者把手指放到感應器時，它會擷取表皮層之下真皮層的高解析度指紋影像，利用導電的電位差測量出紋脊線和凹谷之間的差異。採用電容式技術，只會針對活體判讀有效，也更加準確。在指紋註冊成功之後，蘋果會經由特殊的計算方式，將使用者的指紋數據加密，轉成可比對的模板，它並不儲存在本機的記憶體或傳上網路，而是透過 Secure Enclave 技術，與處理器進行認證配對，保護密碼及指紋資料。蘋果的 iPhone 內有一個 Secure Enclave 晶片，是位於處理器內的協同處理器，通過安全啟動程式，確保每一個軟體都是蘋果驗證的，即使內核出現問題，Secure Enclave 晶片亦能單獨工作，同時每一個 Secure Enclave 晶片的 ID 都是獨立的，就連蘋果公司亦不知道 ID 號碼。裝置啟用時，亦會自動創造一個臨時的密碼與 Secure Enclave 晶片的 ID 結合，防止駭客從軟體及處理器內部中提取用戶的指紋數據。因此蘋果的 Touch ID 感應器會將指紋數據存儲到 Secure Enclave 晶片。

Touch ID 是指紋感應系統，有助於更快、地對裝置進行安全性的存取。可從任何角度來讀取指紋，隨著感應器每次使用時識別出其他重疊的節點而持續擴大指紋圖，逐漸提高對使

用者指紋辨識的能力。Touch ID 讓使用更長、更複雜的密碼變得更為實際，因為使用者無須經常輸入密碼。Touch ID 也克服了以密碼方式鎖定的不便性，它並不會取代密碼鎖定的機制，而是允許在精心設計的範圍和時間限制內，安全地取用裝置。

Touch ID 和密碼

若要使用 Touch ID，使用者必須設定其裝置以要求密碼來將其解鎖。當 Touch ID 掃描並可識別已登記的指紋時，裝置便會自動解鎖，使用者無須輸入裝置密碼。使用者可以隨時使用密碼來取代 Touch ID，並且在以下情況下必須使用密碼：[18]

(1)裝置剛剛開機或重新啟動。

(2)裝置未解鎖的時間超過 48 小時。

(3)裝置收到了遠端鎖定指令。

APPLE ID

Apple ID 是可讓使用 Apple 各項服務的使用者名稱。建立帳號來使用 Apple 服務時，即是建立 Apple ID。以使用同一個 Apple ID 存取 Apple 的其他服務，不需要為每項服務建立新帳號，只需使用 Apple ID 即可。有關於 Apple 帳號安全相關功能如下[14]:[14]：

(1)強式密碼

根據 Apple 政策，Apple ID 必須使用強式密碼。密碼必須至少有 8 個字元，不含超過 3 個連續相同字元，並需要包含數字、大寫字母以及小寫字母。

(2)安全問題

Apple 利用安全問題提供次要的方法來線上識別身分或在聯絡 Apple 支援時使用。

(3)雙步驟驗證

Apple 針對 Apple ID 提供選用的安全強化機制，稱為雙步驟驗證。在更改 Apple ID 中的帳號資訊之前，登入 iCloud 之前，或是從新裝置購買 iTunes、App 或 iBooks Store 的項目之前，雙步驟驗證會要求使用其中一台裝置驗證身分。

(4)加密和 SSL

可以檢視或變更 Apple ID 的所有網頁均採用安全編碼傳輸技術(SSL)來保護隱私。

Keychain 鑰匙圈保護

這項功能可讓 iOS 使用者透過 iOS 設備直接記錄帳號密碼、信用卡資料功能，在開啟這功能後，完全能夠將帳號、密碼儲存至 iCloud 雲端上，這些密碼完全是經過 256 位元 AES 加密保護許多 App 需要處理密碼和其他簡短但較為敏感的資料，如密鑰和登入 Token。

iOS 鑰匙圈[10]提供了儲存這些項目的安全方式。鑰匙圈是以儲存在檔案系統中的資料庫的方式導入。鑰匙圈項目只能在來自同一開發者的 App 間共享。管理方式是要求第三方 App 使用取用群組，並使用透過在 iOS8 中透過應用程式群組來為其分配前置碼。對前置碼的要求和應用程式群組唯一性，是透過程式碼簽署、佈建描述檔和 iOS 強制執行。系統用來保護鑰匙圈項目的類別結構，與檔案資料保護中使用的類別結構相似。這些類別具有與檔案資料保護類別相同的行為，但使用的密鑰不同，所屬 API 的名稱也不同。

可用性	檔案資料保護	鑰匙圈資料保護
未鎖定時	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
鎖定時	NSFileProtectionCompleteUnlessOpen	N/A
首次解鎖後	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
總是	NSFileProtectionNone	kSecAttrAccessibleAlways
密碼已啟用	N/A	kSecAttrAccessible-WhenPasscodeSetThisDeviceOnly

圖 4 iphone 鑰匙圈資料保護加密[24]

對於 iOS 所製作的鑰匙圈項目，將會強制執行下列類別保護：

項目	可取用
Wi-Fi 密碼	首次解鎖後
郵件帳號	首次解鎖後
Exchange 帳號	首次解鎖後
VPN 密碼	首次解鎖後
LDAP、CalDAV、CardDAV	首次解鎖後
社群網路帳號代號	首次解鎖後
Handoff 廣播加密密鑰	首次解鎖後
iCloud 代號	首次解鎖後
家人共享密碼	未鎖定時
「尋找我的 iPhone」代號	總是
語音信箱	總是
iTunes 備份	解鎖時，不可遷移
Safari 密碼	未鎖定時
VPN 憑證	總是，不可遷移
Bluetooth® 密鑰	總是，不可遷移
Apple 推播通知服務代號	總是，不可遷移
iCloud 憑證和專用密鑰	總是，不可遷移
iMessage 密鑰	總是，不可遷移
由設定描述檔所安裝的憑證和專用密鑰	總是，不可遷移
SIM PIN	總是，不可遷移

圖 5 iOS 鑰匙圈對應使用類別[25]

iCloud 鑰匙圈可讓使用者在 iOS 裝置和 Mac 電腦之間安全地同步其密碼，不會將此資訊提供給 Apple。除了的隱私保護和安全性，易用性和回復鑰匙圈的功能對 iCloud 鑰匙圈的設計和架構也具有重要影響。iCloud 鑰匙圈由兩項服務組成：鑰匙圈同步和鑰匙圈恢復。Apple 設計的 iCloud 鑰匙圈和鑰匙圈恢復可確保使用者的密碼在下列情況下仍然受到保護：

(1)使用者的 iCloud 帳號被盜。

(2)iCloud 遭到外部攻擊者或員工入侵。
(3)第三方取用使用者帳號。

鑰匙圈同步

當使用者第一次啟用 iCloud 鑰匙圈時，裝置將建立信任圈並為自己製作同步分身分[19]。同步身分包括專用密鑰和公用密鑰。同步身分的公用密鑰會置於信任圈中，該信任圈已經過兩次簽署：第一次由同步身分的專用密鑰簽署，第二次由來自使用者 iCloud 帳號密碼的非對稱橢圓金鑰簽署。連同信任圈一起儲存的還有參數，用於製作以使用者 iCloud 密碼為基礎的密鑰。已簽署的同步信任圈會置於使用者的 iCloud 密鑰值儲存區域。如果不知道使用者的 iCloud 密碼，就無法對其進行讀取，如果沒有信任圈成員同步身分的專用密鑰，就無法對其進行有效修改。

當使用者在其他裝置上啟用 iCloud 鑰匙圈時，新裝置將在 iCloud 中通知使用者該裝置不是之前已建立的同步信任圈的成員之一。該裝置會製作其同步身分的成對密鑰組，然後製作應用程式申請單以請求加入該信任圈。該申請單包括裝置的同步身分公用密鑰，系統將要求使用者以其 iCloud 密碼進行認證。橢圓密鑰產生參數會從 iCloud 取回並產生用於簽署應用程式申請單的密鑰。最終，應用程式申請單會置於 iCloud 中。當第一部裝置接收到應用程式申請單時，它會顯示一則通知，讓使用者確認新裝置正在請求加入同步信任圈。

鑰匙圈恢復

鑰匙圈恢復包含兩大基本要素：輔助認證和安全託管服務，後者是 Apple 專為支援此功能而建立的服務。使用者的鑰匙圈會使用安全密碼進行加密，只有在滿足一系列嚴格的條件時，託管服務才會提供鑰匙圈拷貝。當 iCloud 鑰匙圈開啟時，系統會要求使用者製作 iCloud 安全碼。恢復託管的鑰匙圈需有此安全碼。依照預設，系統會要求使用者提供簡單的四位數安全碼數值。然而，使用者也可以自行指定較長的代碼或允許其裝置製作加密的隨機密碼，可以自行記錄和保存。

iCloud 家庭成員共享

家人共享群組[3]是一個有隱密性的公開空間，在這裡面，所有成員動向都透明化，成員間可以互相瀏覽對方的私人資訊、檔案資源，有需要時也可自由取用，減少個別傳送的步驟，更為便利。要組織家庭群組需要從設定→iCloud→找到家人共享，由家中任意一位成人從中輸入成員們的 email 帳號，而後系統會發邀請通知給家人；被邀請者按下接受，即完成。

圖 6.iCloud 雲端運用家人共享

家庭共享可容納最多六位家庭成員，只要監護人願意代為申請，13 歲以下兒童也能有自己的 Apple ID；雖然兒童擁有個人 ID，但在家庭群組中一切動向皆有成人看管。Apple 在提供便利同時，同時也對兒童保護。家人共享群組，只要一人購買，所有成員可以一起享受。家庭成員的購買項目會自動出現在每位成員的 iTunes 或 AppStore 已購買標籤中，家人間可以共享 APP，而不需另外付費。啟用家人共享後，手機會自動增加一個 Family 相簿，只要把想共享的照片、影片存到這本相簿，家庭成員在他的手機就能打開，自行挑選使用，可以在相簿中看到其他人添加進來的相片跟影片，同時進行評論。家庭共享的行事曆功能，會同步每個成員家中行事曆帶。家庭共享還有核准購物這一道消費防線。小朋友想趁只要按下購買，系統會立刻傳送核准確認到監護人的手機，決定權將會在監護人身上做最後確認。加入家人共享群組，成員的位置資訊都會自動顯示在尋找我的朋友 App 上。隨時掌握家人行蹤。只要是家庭共享群組內的成員都可以看見對方手機位置。

2. 文獻探討

本章共分為三小節，第 2.1 節將介紹雲端安全聯盟(CSA, Cloud Security Alliance) [16]；第 2.2 節是雲端服務；第 2.3 節是相關雲端文獻探討

2.1 雲端安全聯盟(CSA, Cloud Security Alliance)

雲端安全聯盟(CSA, Cloud Security Alliance)成立於 RSA Conference 2009，為全球

性的非營利組織 致力於在雲端運算環境下提供最佳的安全方案。自其成立起，雲端安全聯盟發佈的雲端安全指南及其開發成為雲端運算領域令人矚目的重要文件，雲端安全聯盟發佈了新版的《雲端安全指南 v3.0》[4]，指南中代表著雲端運算和安全業界對於雲端運算及其安全保護的認識。

雲端安全聯盟 CSA 的宗旨：

(1)提供用戶和供應商對雲端運算必要的安全需求與資安認知。

(2)促進對雲端運算安全最佳做法的獨立研究

(3)發起正確使用雲端運算和雲端安全解決方案的宣傳和教育計畫

(4)創建有關雲端安全保證的問題和方針的明細表。

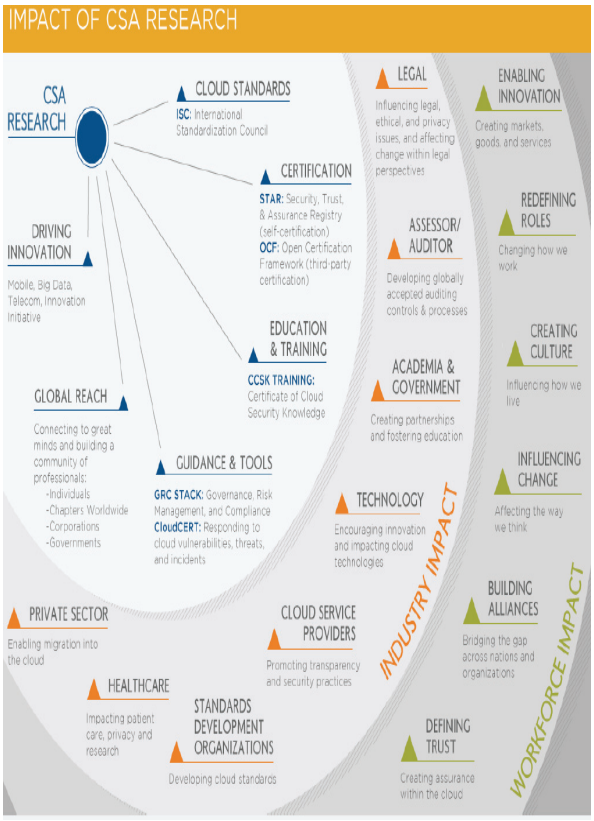

圖7 CSA 雲端資訊安全應用領域影響因子[16]

行動化

強化軟體與部署到實體行動裝置的安全分析行動裝置的作業系統與操作上的安全問題以雲端為基礎的管理架構、配置、政策以及資料的管理，以實現全方位的管理機制。解決 BYOD 對於企業的影響，包括個人或是企業所擁有行動裝置軟體開發的最佳實例。

大數據

定義可擴展的技術，以應用在資料中心的安全以及隱私的問題創建最佳的實踐，以應用在資安與隱私權的巨量資料分析協助產業與政府採用最佳的做法與其它的組織建立聯繫，以協調發展巨量資料分析與隱私資料的保護標準加速新的研究，目標以解決資料安全與隱私的議題。

隱私權協議準則

2013 年 2 月發佈雲端供應商隱私權協議準則在 PLA 的議題中(傳統的作法僅採用服務水準協議)，雲端服務供應商需清楚的定義對於隱私資訊的保護與資料儲存的保護程序提供雲端服務的用戶相關工具，以量測與驗證雲端服務供應商對於個人資料保護的承諾 提供合約與協議的參考，以確保雲端服務供應商與用戶之間的關係，包括對於隱私資訊與資料保護的作法。

雲端服務威脅

該協會定義出目前雲端最常發生的資安事件，經過整理一共有八項，條列出以下的事件：

(1)資料洩露。

(2)資料遺失。

(3)帳戶劫持。

(4)不安全的阻斷服務。

(5)惡意的內部人員。

(6)濫用與惡意的使用。

(7)未盡職責的調查。

(8)共享技術的議題。

2.2 雲端服務

雲端運算的名詞最早是由 Google 提出[2]，但此概念並非由 Google 獨創，目前所熟知的雲端運算也是經由過去一連串如網格運算、公用運算等技術逐漸演進而來。廣義來說，任何網際網路上提供的運算資源和隨選服務都是雲端運算服務的涵蓋範圍，只要滿足彈性使用和可擴充的特性，並不一定需要完全符合分散式電腦運算架構。在多方闡述中，事實上以美國國家標準與技術研究院(NIST)[5]最具權威，其雲端定義為：雲端運算是一種模式，能方便且隨需求應變地透過連網存取廣大的共享運算資源，並可透過最少的管理工作及服務供應者互動，快速提供各項服務。NIST 提出的定義中，也進一步說明雲端運算的四種佈署模式、三類服務模式、以及五項重大特徵以及一般特性，其整體架構如下圖：

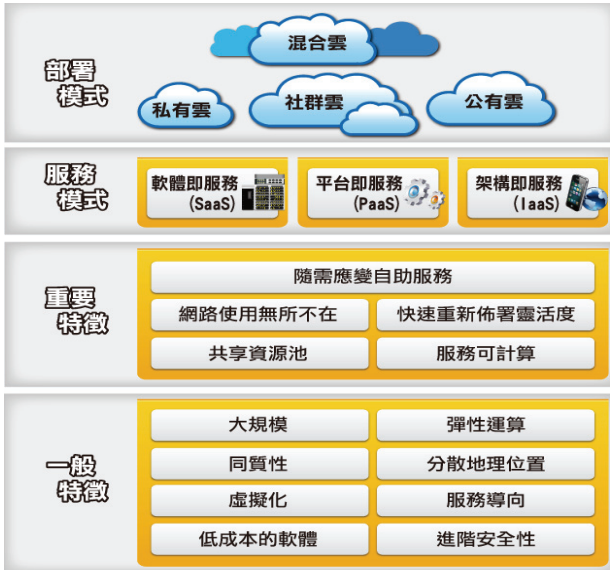

圖 8 美國國家標準與技術研究院雲架構[15]

重點特徵

依據 NIST(National Institute of Standards and Technology, 美國國家技術標準局)所定義的內容[5]，雲端運算有五大重點特徵：

(1)隨需應變自助服務(On-demand Self-service)

消費者可依據使用需求狀況自行使用雲端服務，不需再透過雲端供應者與之互動。

(2)網路使用無所不在(Broad Network Access)

網路使用無所不在，亦即雲端供應者服務可隨時在網路取用，且使用者端無論大小，均可透過標準機制使用網路。

(3)共享資源池(Resource Pooling)

資源彙整讓雲端供應者透過多租戶模式(Multi-tenancy)服務消費者，依據消費者要求，來指派或重新指派實體及虛擬資源，在所在地獨立性的概念下，消費者通常不知道所有資源確切位置，只可能掌握國家、州或資料中心等大範圍區域地點。其中資源包括儲存、處理、記憶、網路頻寬和虛擬機等。

(4)快速重新佈署靈活度(Rapid Elasticity)

彈性亦即能因應需求彈性且快速調整資源規模大小，對消費者而言，所提供的這種能力似乎是無限的，可以在任何時間被購買任何數量。

(5)服務可計算(Measured Service)

計算服務量測中，雲端服務各層次均由雲端供應者掌控與監管，這對於計費、存取控制、資源優化、處理能力規畫及其他工作相當重要，確保資源使用可被監測、被控制和被報告，為供應者和消費者雙方提供透明化服務使用資訊。

服務模式

根據 NIST 定義[5]，雲端服務架構可依服務類型指標劃分為基礎架構、平台以及應用三大層次，分別為基礎架構即服務(IaaS)、平台即服務(PaaS)以及軟體即服務(SaaS)。所謂服務類型是指雲端運算能為使用者提供什麼樣的服務，而透過這樣的服務能讓使用者獲得哪些資源，以及用戶如何運用這樣的服務。分別介紹如下：

圖 9 雲端服務架構圖[15]

(1)基礎架構層(IaaS)，即基礎架構即服務，是虛擬化後的硬體資源和相關管理功能的集合，透過虛擬化技術將運算、儲存和網路等資源抽象化，實現內部流程自動化和資源管理優化，進而向外部提供動態、靈活的基礎架構服務。此層的消費者使用處理能力、儲存空間、網路元件或中介軟體等基礎運算資源，還能掌控作業系統、儲存空間、已部署的應用程式及防火牆、負載平衡器等，但並不掌控雲端的底層架構，而是直接享用 IaaS 帶來的便利服務。

(2)平台層(PaaS)，即平台即服務，為雲端應用提供了開發、運行、管理和監控的環境，可說是優化的雲端中介軟體，優良的平台層設計可滿足雲端在擴充性、可用性和安全性等方面的要求。此層的消費者可透過平台供應商提供的程式開發工具來將自身應用建構於雲端架構之上，雖能掌控運作應用程式的環境，但並不掌控作業系統、硬體或運作的網絡基礎架構。

(3)應用層(SaaS)，即軟體即服務，是軟體的集合，這些應用架構於基礎架構層提供的資源以及平台層提供的環境之上，並透過網路交付給用戶。此層提供的應用可讓其使用者透過多元連網裝置取用服務，僅需打開瀏覽器或連網介面即可，不再需要擔心軟體的安裝與升級，也不必一次買下軟體授權，而是根據實際使用情況來付費。而對應用開發者來說，可以方便地進行軟體部署和升級，不需管理或控制底層的雲端架構，例如網路、伺服器、作業系統、儲存等。

部署模型

雲端運算按照供應商和使用者所屬關係可分為四大類，即公用雲、私有雲、社群雲和混合雲[5]。分別說明如下：

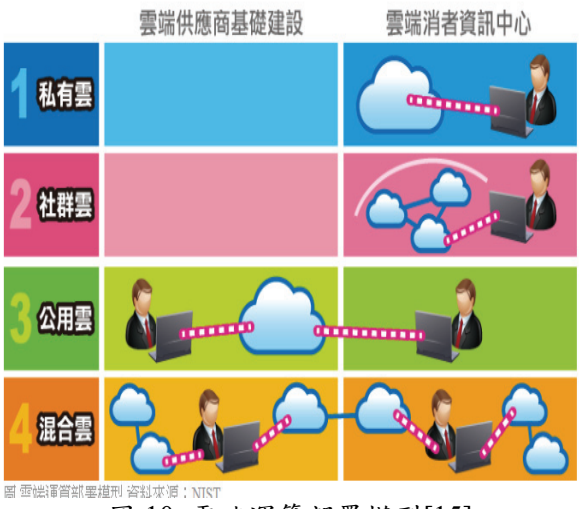

圖 10 雲端運算部署模型[15]

私有雲(Private Cloud)：雲基礎設施專為組織而運作，這可能是由組織本身或第三方管理者就地部署或遠端部署。其中，私有雲除具備公用雲環境的彈性優點，還能因網路與使用者受到特殊限制，且資料與程序皆在組織內部管理，較不受網路頻寬、安全疑慮、與法規限制等影響，讓雲端供應者及使用者更能掌控雲端基礎架構並改善安全與彈性。

社群雲(Community Cloud)：雲基礎設施由眾多利益相仿的組織掌控及使用，社群成員可共同使用雲端資料及應用程式，擁有共同的關注問題，例如特定任務、安全要求、政策考量等。可能由組織或第三方管理，且可以就地部署與遠端部署。

公用雲(Public Cloud)：雲基礎設施提供給一般大眾或一個大產業集團，由銷售雲服務的組織所擁有，除彈性之外，又能具備成本效益。其中公用一詞並不代表絕對的免費，但也可能代表免費或相當廉價，另外公用並不表示使用者資料可供任何人查看，雲供應者通常會對使用者實施使用存取控制機制。

混合雲(Hybrid Cloud)：雲基礎設施是由兩個或兩個以上組成的雲(私有、社群或公用)，此種雲維持單一實體，但是藉由標準或專有技術聯繫在一起，使資料和應用程序具可移植性。此類這個模式中，使用者通常將非企業關鍵資訊外包，並在公用雲上處理，但同時掌控企業內部機敏服務及資料。

2.3 相關雲端文獻探討

本章節透過相關歷年相關雲端文獻探討，可以知道目前雲端服務的使用廣泛度，及在使用資料儲存的時候，與本地儲存優缺點，以及歷年重大雲端服務資安事件。

2.3.1 iOS 裝置控制

Jitendra Singh[8]有針對雲端服務的優缺點做出比較與討論，其他熱門使用的雲端系統，如 google driver、dropbox、iCloud 等，作者提到市面上的雲端軟體使用者最需要考量的兩個問題就是資安與可用性。

Jitendra and Ashish[8]也提到雲端儲存服務會是未來的趨勢，會取代傳統的一般電腦本機儲存習慣，在使用者使用經驗下考量的是雲端服務的可用性、價格、與安全性，雲端儲存有如下幾個優點：

(1) 可以在有網路的環境下隨時存取：
取代現有的隨身碟，只要有網路就可以隨時存取網路檔案。

(2) 可作異地備援的資料保全：
不怕電腦硬碟掛了造成文件的資料匣內容不見。

(3) 網路分享：
可與信任的使用者，共享同個資料匣。

(4) 支援行動裝置：
舉凡 iOS，、Android 或是 WindowsPhone，都有相關配套可以瀏覽或下載檔案。

2.3.2 歷年重大雲端軟體服務資安事件

Rachna Jain [12]提出各大知名雲端軟體有發生過資安事件，可不得不讓人在使用雲端軟體的時候需要注意資安考量，以下列出知名事件

Dropbox

發生時間 2011/06 根據 Dropbox 官方的確認，在太平洋時間下午 1:54 到 5:46 分的時間，其服務的使用者可以任意的密碼登入 Dropbox，也就是說在將近四個小時的時間裡，用戶帳號被放置在具有極大潛在危險的情況下。由於 Dropbox 的帳號是使用用戶的 email，這表示，你可以登入任何你擁有 email 的 Dropbox 帳戶，Dropbox 的工作人員表示，目前他們評估受到影響的人數約為總帳戶數的 1%。

Microsoft Business Productivity Online Suite

發生時間 2010/12 微軟企業生產力線上套件配置錯誤，導致暴露了用戶聯繫人的通訊簿

資訊給其他客戶。

GoGrid

發生時間 2011/03 可能是透過第三方軟體洩漏了使用者帳號資訊，包含了信用卡資訊。

AppleiCloud

發生時間 2014/09 iCloud 爆發私人照片遭駭客竊取並散布的事件，於 iCloud 上的照片全被駭客破解密碼，並且將檔案存放於其他網路空間、散佈在網路上表示一向注重個人隱私與資安問題的蘋果公司，居然出現這樣的漏洞，覺得相當不可思議。iCloud 洩密事件其實有駭客在 Github 上公開 iCloud 暴力破解工具，讓一些設定較簡單密碼在幾萬次的嘗試下進行暴力破解的動作，這是毫無技術困難度的攻擊，AppleiCloud 沒有任何告警機制，而後續的明星私人照片陸續外洩而被公開時，讓雲端存放資料的安全問題又再度讓使用者失去信心。

Sony PlayStation Network

發生時間 2011/4 索尼(Sony)PlayStation Network(PSN)在 4 月 20 日遭駭客入侵，被竊取 7 千 7 百萬筆 PS3 及 Qriocity 音樂隨選服務使用者的個人資料;在 5 月 3 日又被揭露,Sony 旗下線上遊戲子公司網站 Sony Online Entertainment(SOE)有 2,460 萬筆個人資料遭到駭客竊取。

至於飽受爭議的信用卡資料是否外洩，Sony 先前 7,700 萬筆的外洩個資中，仍未確認其中 1 千萬筆信用卡資料是否外洩，但在線上遊戲 SOE 外洩的資料中,則確認駭客成功取得 23,400 筆、從 2007 年後逾期的信用卡資料，美國以外有 12,700 筆的信用卡卡號及有效日期資料遭竊。

Sony 迄今遭到外洩的個資已經超過 1 億筆，外洩個資內容包括用戶名稱、地址、電子郵件信箱、生日、性別、電話號碼、帳號、密碼等，甚至有外電報導，連 PSN 安全提問的問題也在外洩資料之列。Sony 在第一波暫停 PSN 服務大約 3 天後，才對外公布個資外洩的事實。該起事件不僅外洩了用戶的帳號、密碼、住址、電子郵件等，甚至還包括了重要的信用卡號，受害人數直逼上億。

Xbox Live

發生時間 2014/3 美國加州聖地牙哥市一男童 Kristoffer Von Hassel，年僅 5 歲講話還有些不太清晰，竟然與多位資安專家一起名列微軟 3 月份資安通報有功的研究員，因為他發現了躲避 Xbox Live 帳號檢查的方法。目前微軟已經修補了這個程式漏洞。

Twitter Breach

發生時間 2013/2 資訊安全主管 Bob Lord 表示，該網站偵測到異常現象，有不知名人士試圖取得用戶資料，雖然該網站立即採取措施，仍懷疑 25 萬名使用者資料可能已經外洩。隔日 Twitter 發出電子郵件警告這些用戶，告知使用者帳戶已遭非 Twitter 相關的網站或服務所盜用，並已經直接變更使用者密碼，要求使用者依照標準流程重新設定密碼。

2.3.3 在智慧型手機上使用者安全知覺探討

之前 Erika Chin[6]提出,使用者在使用智慧型手機的時候,會因為使用裝置的不同而有不同的安全認知,特別是桌上型 PC 與手持裝置有明顯的差異性。

3. iCloud 安全性分類

本章分兩節，第 3.1 節討論 iOS 安全性，第 3.2 節針對 iCloud 安全性做分類，並且提出安全性設定建議。

3.1 iOS 系統安全性

系統安全性旨在確保每部 iOS 裝置的所有核心元件都能為軟體和硬體提供安全保護。這包含啟動程序、軟體更新和 Secure Enclave。此架構是 iOS 安全性的核心並不會影響裝置的正常使用。iOS 裝置的硬體和軟體經過緊密的整合，可確保系統的每個元件獲得信任，並對系統整體進行驗證。從初次啟動到 iOS 軟體更新、再到第三方的 App，每個步驟都經過分析和審查，以確保硬體和軟體以最佳方式協同執行，並適當地使用資源。安全啟動鏈啟動程序中每個步驟包含的元件都經過 Apple 加密簽署以確保其完整性，且只有在驗證信任鏈結後，每個步驟才能繼續。這包含 bootloader、核心、核心延伸功能和韌體。開啟 iOS 裝置後，其應用程式處理器會立即執行唯讀記憶體中的程式碼。此類無法更改的程式碼是在製造晶片時完成設定，且已間接獲得信任。

iOS 加密與資料保護

安全啟動鏈、程式碼簽署及執行階段程序安全性都有助於確保，只有受信任的程式碼與 App 可在裝置上執行。iOS 還有其他加密與資料保護功能可保護使用者資料的安全，即使是安全性基礎架構的其他部分遭到破壞。這對於使用者與 IT 管理者都大有助益,可隨時保護個人與企業的資訊，並提供裝置遭竊或遺失時，於遠端立即完全清除的方式。

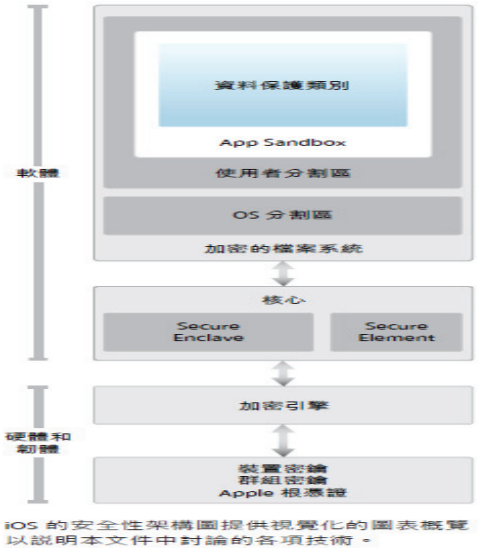

圖 17 iOS 安全性架構圖[20]

除了 iOS 裝置內建的硬體加密功能，Apple 也使用名為資料保護的技術，進一步保護儲存於裝置快閃記憶體中的資料。資料保護可讓裝置回應如來電之類的常見事件，也可以對使用者資料啟用較高層次的加密。訊息、郵件、行事曆、聯絡資訊、照片和健康資料值等主要系統 App 預設都會使用資料保護，而安裝於 iOS7 或更新版本上的第三方 App 可自動獲得此項保護措施。檔案系統中所有檔案的元資料都使用隨機密鑰進行加密，該密鑰是在首次安裝 iOS 或使用者清除裝置時製作而成。檔案系統密鑰則儲存在 Effaceable Storage 中。因為該密鑰儲存在裝置上，因此它不是用來維護資料的機密性，而是可以視需求快速清除，或者由使用者或管理者從行動裝置管理(MDM)伺服器、Exchange ActiveSync 或 iCloud 發出遠端清除指令來清除[23]。以此方式清除密鑰將會透過加密的方式讓裝置上的所有檔案無法取用。檔案的內容使用檔案專屬密鑰進行加密，該密鑰使用類別密鑰封裝並儲存在檔案的元資料中，檔案元資料接著又使用檔案系統密鑰進行加密。類別密鑰使用硬體 UID 取得保護，而某些類別則透過使用者密碼取得保護。此階層架構同時提供了彈性與效能。例如，更改檔案的類別只需要重新封裝其檔案專屬密鑰，更改密碼只需要重新封裝類別密鑰。

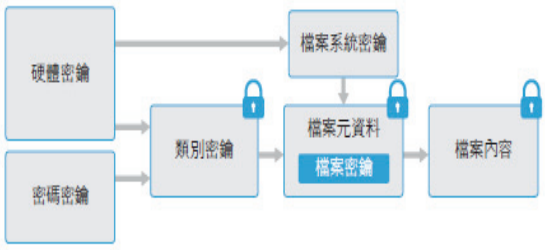

圖 18 iOS 系統加密模型[21]

iOS App 安全性

App 是現代行動安全架構最關鍵的要素之一。雖然 App 可顯著提高使用者的生產力，但若處理不當，也可能對系統安全性、穩定性和使用者資料產生負面影響。有鑑於此，iOS 提供了多重保護來確保 App 經過簽署和驗證，且以 Sandbox 技術限制，進而保護使用者資料。這些要素為 App 提供了穩定且安全的平台，讓成千上萬的開發者能夠在 iOS 上提供數十萬款的 App，而不會影響系統的完整性。使用者可以在其 iOS 裝置上取用這些 App，無須過度擔心病毒、惡意軟體或未經授權的攻擊。

App 程式碼簽署

一旦 iOS 核心啟動後，它將控制可執行哪些使用者程序和 App。為了確保所有 App 均來自核准的已知來源且未被竄改，iOS 會要求所有可執行的程式碼均使用 Apple 核發的憑證進行簽署。裝置所隨附的 App 則由 Apple 簽署。第三方 App 也必須使用 Apple 核發的憑證進行驗證和簽署。強制性程式碼簽署將信任鏈的概念從作業系統延伸至 App，可防止第三方 App 載入未簽署的程式碼資源，或使用自行修改的程式碼。

延伸功能

iOS 可允許 App 透過延伸功能來對其他 App 增加功能。延伸功能是具有特殊用途的已簽署可執行二進位程式碼，封裝在 App 內。系統會在安裝時自動偵測延伸功能，並讓使用相符系統的其他 App 使用這些延伸功能。支援延伸功能的系統區域稱為擴充點。每個擴充點都提供 API，並為該區域強制執行規則。系統依據擴充點特定的比對規則來決定哪些延伸功能可供使用。系統會自動視需要啟動延伸功能程序，並管理它們的生命週期。授權可用來限制特定系統應用程式的延伸功能可用性。例如，今天顯示方式 Widget 只顯示在通知中心內，而共享的延伸功能則只能從共享面板中使用。擴充點有 Widget、分享、自定動作、照片

編輯、文件提供程式和自定鍵盤。延伸功能會在其自己的位址空間中執行。App 與其啟動的延伸功能之間的通訊使用由系統架構所協調的程序間通訊。它們無法存取彼此的檔案或記憶體空間。延伸功能的設計旨在將它們彼此區隔、與其包含的 App 區隔，並且與使用它們的 App 加以區隔。與其他第三方 App 類似，它們也以 Sandbox 技術限制，且擁有的容器會與包含 App 的容器隔開。不過，延伸功能與其容器 App 對隱私控制具有相同的存取權限。因此，若使用者對 App 授予聯絡資訊的存取權限，該 App 中嵌入的延伸功能也會獲得此許可權，但由 App 啟動的延伸功能則不具有該許可權。

iOS 網路安全

除了 Apple 用於保護 iOS 裝置上所儲存資料的內建安全保護，也有許多網路安全措施可供企業組織採用並確保資訊從 iOS 裝置來回傳輸時安全無虞。行動使用者必須能在全球各處存取公司網路，因此很重要的一點是確保獲得授權並且其資料在傳輸期間受到保護。iOS 使用標準網路通訊協定並使開發者能夠存取這些通訊協定，以進行受認證、已授權且已加密的通訊。為了達成這些安全性的目標，iOS 整合了經過實證的技術和最新標準來進行 Wi-Fi 和行動數據網路的連線。在其他平台上，需要用防火牆軟體來保護開放式通訊埠，以防止入侵。因為 iOS 透過限制監聽埠以及移除不必要的網路工具程式，使受攻擊的範圍減小，因此在 iOS 裝置上不需要額外的防火牆軟體。

iOS 網際網路服務

Apple 已內建一套強大的服務來協助使用者更充分地使用裝置並提高生產力，其中包含 iMessage、FaceTime、Siri、Spotlight 建議、iCloud、iCloud 備份和 iCloud 鑰匙圈。這些 Internet 服務都具備了 iOS 在整個平台上推動的安全性目標。這些目標包含資料的安全處理，無論是裝置上儲存的靜態資料或是透過無線網路傳輸的資料；保護使用者的個人資訊；以及對資料和服務的惡意或未經授權的存取威脅加以防護。每項服務在使用其本身的強大安全性架構時，絲毫不影響 iOS 整體的易用性。

iOS 裝置控制

iOS 支援具彈性的安全性原則和設定，讓使用者容易實施並管理。這可讓各機構保護公司資訊並確保員工遵守企業要求。例如，作為員工自攜裝置(BYOD)計畫的一部分，員工甚至可以使用自己攜帶的裝置。公司可以使用密碼保護、設定描述檔、遠端清除和第三方 MDM 解決方案等資源來管理裝置流通並協助確保公司的資料安全，甚至在員工使用私人的 iOS 裝置取用資料時，亦能保障安全。

3.2 iCloud 安全性分類

本節將 iCloud 的關於安全性的部分做出分類[1]，並且根據網路上的參考資料[16][17][23]提出安全的與使用建議。

項目	建議設定
使用裝置驗證	我的 Apple ID->管理 Apple ID->密碼與帳號安全在雙步驟驗證底下，選取開始設定，然後按照螢幕上的指示操作
個人資料保護	開啟自動刪除密碼錯誤超過 10 次以上刪除所有資料
	開啟遠端刪除遠端控制是否刪除裝置之所有資料
	開啟遠端定位遠端控制定位裝置之目前位置
	遺失模式位置資料僅會要求時才透過裝置傳送，任何其他時間並不會傳送或記錄位置資料,最近一次的裝置位置資料會以加密格式儲存在 Apple 的伺服器上 24 小時，之後就會永遠刪除
	遠端鎖定遠端清除功能可永久且安全地清除裝置的資料
iCloud 鑰匙圈	規範信任設備 只有經過核准的受信任裝置才能存取 iCloud 鑰匙圈。 設定->iCloud->鑰匙圈
	設定安全碼 使用進階設定選擇長度超過四位數的 iCloud 安全碼。
	停用鑰匙圈 停用鑰匙圈恢復功能，也就使遍及核准裝置中的 iCloud 鑰匙圈保持最新狀態，但不會儲存已加密的資料。 設定->iCloud->鑰匙圈。
照片隱私	我的照片串流 將不要的照片從我的照片串流中刪除
	共享照片 將不要的照片和影片從共享的相簿中刪除

	訂閱者 將訂閱者從所建立的共享相簿中移除
	iCloud 照片共享 使用家人共享，會自動加入 iCloud 照片共享家庭成員共享相簿。可以控制要分享哪些照片、影片以及評論
位置共享	共享位置 使用家人共享，可以選擇是否和家庭成員共享裝置的位置資訊。預設為不會共享裝置的位置資訊。位置只有在朋友要求查看裝置位置，或選擇在訊息中傳送目前位置時，才會從裝置傳送出去
	尋找我的朋友 使用尋找我的朋友 App 或 iOS8 內建的訊息 App，與朋友和家人分享位置若要讓某人查看裝置位置，必須先授予這個人權限
	分享我的位置 向所有好友隱藏置按下一個開關即可，最近一次的已知位資料會在 Apple 的伺服器上以加密格式只儲存 2 小時，之後就會永遠刪除。
Touch ID	與免責聲明要詳細閱讀 APP 安裝時的告警內容與免責聲明
	使用 Touch ID 加解密手機鎖

表一 iCloud 安全性分類一覽表

4. 結論與未來展望

隨著智慧手機的發展，行動上網裝置越來越普及。隨著智慧型手機的普及過去以本地端儲存為主的使用習慣，漸漸被雲端服務所取代。過去行動裝置使用者多半習慣將照片、影片、文檔等資料，存放在隨身碟上，以便攜帶至不同的電腦上，進行這些檔案的分享。現在只需要透過網路連結，就可以將這些需要被分享、或是有待存取編輯的資料，放在遠端主機上，在有需要取用時，就能透過網路的連線進行下載，保持資料維持在最新版本。當然，雲端服務另一個重要的優勢，就是支援了多裝置的同時存取，在使用上更具彈性。然而隨著雲端服務的便利性，衍生出來的就是使用者資安認知的使用問題。針對 iCloud 服務的安全選項作詳細探討，正確安全的使用 iCloud 雲端服務需要透過完整持續的教育訓練來達成目的。本論文透過研究標的 iCloud 雲端服務的安全控制措施依照性質進行分類整理，提出實際使用時的安全設定建議，能讓使用者在使用便利的雲端服務，能相對安全的使用環境，在安全性的設定上提供更進一步的參考，以增加個人資訊的防護，降低可能的風險。

展望未來，透過持續教育訓練來加強使用者的安全意識與認知，讓使用者對 iCloud 雲端服務設定熟悉。從雲端服務的觀點來看，建議雲端服務使用者在使用便利的 iCloud 雲端服務的同時，透過教育訓練的方式讓使用者提高相對應正確的資安風險意識。

參考文獻

[1] 行政院研究發展考核委員會，101 年度行動裝置資安防護參考指引， 2012。

[2] 江政哲、張迺貞，“初探雲端運算”，***海峽兩岸圖書資訊學學術研討會論文B輯***，第32-52頁，2012。

[3] 行動裝置是否安全引發疑慮 - 行政院國家資通安全會報技術服務中心 http://www.icst.org.tw/NewsRSSDetail.aspx?seq=13989。

[4] Ally, M., and Gardiner, M. “The moderating influence of device characteristics and usage on user acceptance of smart mMobile devices,” ***Proceedings of the 23rd Australasian Conference on Information Systems 2012*** pp. 1-10, 2012.

[5] CSRC With The NIST Definition of Cloud Computing. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[6] Chin, E., Felt, A. P., Sekar, V., and Wagner, D., “Measuring user confidence in smartphone security and privacy,” ***In Proceedings of the Eighth Symposium on Usable Privacy and Security*** pp1. , 2012.

[7] Furnell, S. M., Bryant, P., and Phippen, A. D., “Assessing the security perceptions of personal Internet users,” ***Computers & Security***,Vol 25 ,No. 5, pp.410-417, 2007.

[8] Singh, J., and Jha, A. “Cloud storage, issues and solution,” ***International Journal of Engineering and Computer Science ISSN***, pp.2319-7242, 2014.

[9] Mylonas, A., Kastania, A., and Gritzalis, D., “Delegate the smartphone user security awareness in smartphone platforms,” ***Computers & Security***, Vol. 34, pp.47-66, 2013.

[10] 瘋先生：iPhone/iPad 教你使用 iOS7 上的所有密碼儲存至 iCloud 功能。 http://mrmad.pixnet.net/blog/post/165943515-Biphone-ipad

[11] New security flaws detected in mobile devices. http://usatoday30.usatoday.com/tech/news/story/2012-04-08/smartphone-security-flaw/54122468/1

[12] Rachna J., Gaurav S., and Anuj M., “Survey on security issues in cloud computing environment,” ***International Journal of Innovative Research in Computer and Communication Engineering*** Vol. 2, No. 11, 2014.

[13] 蘋果公司我的照片串流 FAQ。 https://support.apple.com/zh-tw/HT201317

[14] 蘋果公司 Apple ID 雙步驟驗證問題。 http://support.apple.com/zh-tw/HT204152

[15] 雲端知識庫。 http://www.cloudopenlab.org.tw/

[16] CSA 簡介 — 台灣雲端安全聯盟。 http://www.twcsa.org/about1/

[17] 蘋果公司 iOS 安全性白皮書。 https://www.apple.com/tw/business/docs/iOS_Security_Guide.pdf.

[18] 蘋果公司 iOS 安全性白皮書。 https://www.apple.com/tw/business/docs/iOS_Security_Guide.pdf.

[19] 蘋果公司 iOS 安全性白皮書。 https://www.apple.com/tw/business/docs/iOS_Security_Guide.pdf.

[20] 蘋果公司 iOS 安全性白皮書。 https://www.apple.com/tw/business/docs/iOS_Security_Guide.pdf.

[21] 蘋果公司 iOS 安全性白皮書。 https://www.apple.com/tw/business/docs/iOS_Security_Guide.pdf.

[22] 蘋果公司 iCloud - Apple 。 http://www.apple.com/tw/icloud/

[23] 蘋果公司 iOS 安全性白皮書_2014 年份， https://www.apple.com/tw/privacy/docs/iOS_Security_Guide_Oct_2014.pdf.

[24] 蘋果公司 iOS 安全性白皮書_2014 年份。 https://www.apple.com/tw/privacy/docs/iOS_Security_Guide_Oct_2014.pdf.

[25] 蘋果公司 iOS 安全性白皮書_2014 年份。 https://www.apple.com/tw/privacy/docs/iOS_Security_Guide_Oct_2014.pdf.

[26] The Year's Worst Hacks, From Sony to Celebrity Nude Pics WIRED . http://www.wired.com/2014/12/top-hacks-2014/

[27] iCloud - 維基百科，自由的百科全書。 https://zh.wikipedia.org/wiki/ICloud