《育 達 科 大 學 報》
第 5 期，民國 100 年 6 月
Yu Du Academic Journal
Vol.5, June 2011

企業導入雲端運算的技術解決方案-四個案例

林開榮 *　　謝東盛 **

育達商業科技大學資訊管理系(所)副教授兼系主任(所長)*
(linky@ydu.edu.tw)
育達商業科技大學資訊管理系(所)碩士班研究生**
(98104505@ydu.edu.tw)

摘要

雲端運算的虛擬化技術可以說是 IT 界中最先進的技術。然而，目前企業在導入雲端運算時，多數會遭遇到各種問題，這些問題將會影響雲端運算的發展，且致使雲端運算無法成為一個新的資訊趨勢。在本文中，我們提出了雲端運算目前所面臨的各種資安問題。除此之外，同樣重要的是，本文描述了幾個已導入雲端運算的企業案例，藉由案例所使用方解決方案，來減少使用者因使用雲端運算所產生的疑慮。同時藉由不斷的改進導入雲端運算所遭遇到的問題，來促使雲端運算此項新技術可以普遍的讓企業運用，進而取代複雜的資訊系統建構，且融合到日常生活中來使用。

關鍵字：雲端運算、雲端解決方案、雲端案例

壹、緒論

1.1、研究背景

整個電腦發展史，從早期「超級電腦/大型電腦」、近期「個人電腦」，將邁入以超大規模數量電腦主機虛擬集結的「雲端運算」時代。雲端運算將電腦集中運用，未來電腦運算設施就像是水、電；資料儲存與應用就像是銀行，只要連上網路就可以使用，不必各自投資發展。「雲端運算」未來將成爲每個國家的重要基礎建設。

我國資訊及通訊產業經過數十年的發展，已經成爲全球重要的硬體資訊產品供應基地，但雲端運算讓電腦運算資源改以服務形式，經由網際網路直接取得，重新塑造資訊產業供應鏈，全球資訊產業重新洗牌，引發新一波的競爭局

1.2、研究動機與目的

本研究主要目的希望除了依靠雲端服務供應商所提供的資訊安全防護外，企業與使用者本身能夠具有基本的防護機制，而這樣的機制既不會造成在雲端服務無法使用，又可以保護企業儲存在雲端的資料，若雲端服務供應商無法提供足夠的安全性服務或服務中斷時，企業能夠具有因應措施，使災害能降至最低。同時獲得最佳的解決方案，且能達到安全的資料保護。

貳、何謂雲端運算

雲端運算(cloud computing)從 2008 年開始就是一個熱門的話題，對於雲端運算的定義，它究竟是一種「技術」或「概念」，到底是「產品」還是「服務」，無論是應用程式服務、資安服務或資料儲存等，各家都有不同的說法與見解，但從資安的觀點來看，仍有一些地方值得企業審慎注意。在此我們僅從資訊安全的角度，來探討雲端運算可能帶來的資安問題或風險，以做爲企業導入雲端運算的參考。

2.1、雲端運算的定義

究竟什麼是雲端運算，Gartner 定義它是一種嶄新且具延展性的運算方法，可以將計算、儲存等資訊科技的運用，透過網路以服務方式提供給外部客戶使用。而維基百科則說，「雲端運算是一種基於網際網路的運算新方式，透過網際網路上的服務爲個人和企業使用者提供所需即取的運算。」

雲端運算並非全新概念，從早期網格運算（Grid Computing）、公用運算（Utility Computing）、到軟體即服務（SaaS）的逐步演進，發展出新一代網路服務與資料中心。雲端運算之所以逐漸受到重視，網路的普及、頻寬的大幅提升、虛擬化、Web

2.0 的互動和即時溝通等技術之成熟，爲雲端運算提供極大的助力(如圖 2.2.1 所示)。

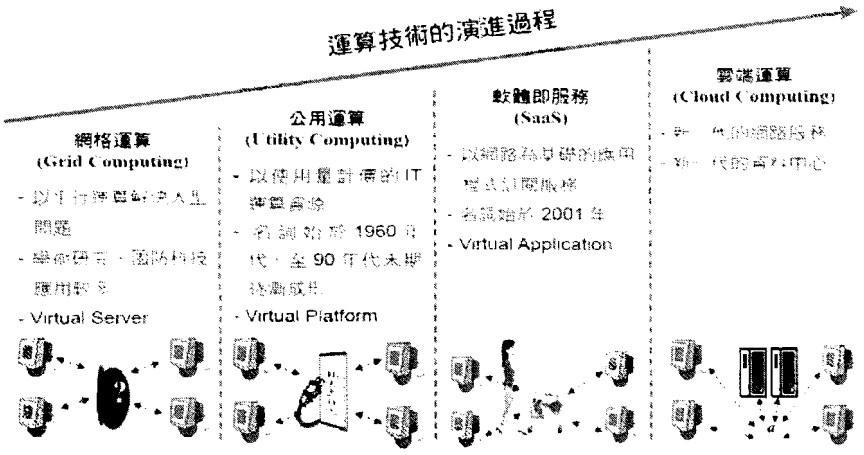

圖 2.1.1 運算技術的演進過程

首先，讓我們回憶一下，在還沒有所謂的雲端運算之前，企業對於資訊的處理與運作的方式是什麼？一般普遍性的作法是，企業需要自行添購或開發商務運作所需要的軟體和硬體，並且建置專屬的資訊機房和網路環境，然後由內部的資訊人員來執行維運等相關工作。

對大多數的企業而言，隨著營運規模的擴展，爲了要增加資訊服務的穩定與效率，在資訊科技的費用支出相對也會節節升高，尤其是面對如今愈來愈複雜的網路環境與技術，再加上好的資訊人才難尋，和營運相關的資訊問題解決能力也需要時間培養，種種問題都讓企業主傷透腦筋，而「雲端運算」的出現，彷彿就像是在烏雲之中露出了一道曙光。

2.2、雲端運算的資安服務

基本上，雲端運算是處理與分享大量資料的一種 IT 基礎架構，把眾多電腦系統連結成大型資源庫，以提供 IT 應用服務。雲端運算的精神是強調服務，並能依照使用者的需求提供客製化服務，也就是說：將所有的應用服務、電腦與網路資源（如資料庫儲存量、網路速度等），都以如使用水和電等公用事業服務的方式提供給使用者，並依使用者的需求隨時取用，可按次、按量或按時計費。

目前，雲端運算具備三大運算架構模式，包括了基礎架構即服務（Infrastructure as a Service，IaaS）、平台即服務（Platform as a Service，PaaS）及軟體即服務（Software as a Service，SaaS）等，當然還有人提供許多不同的服務(如圖 2.2.1 所示)。

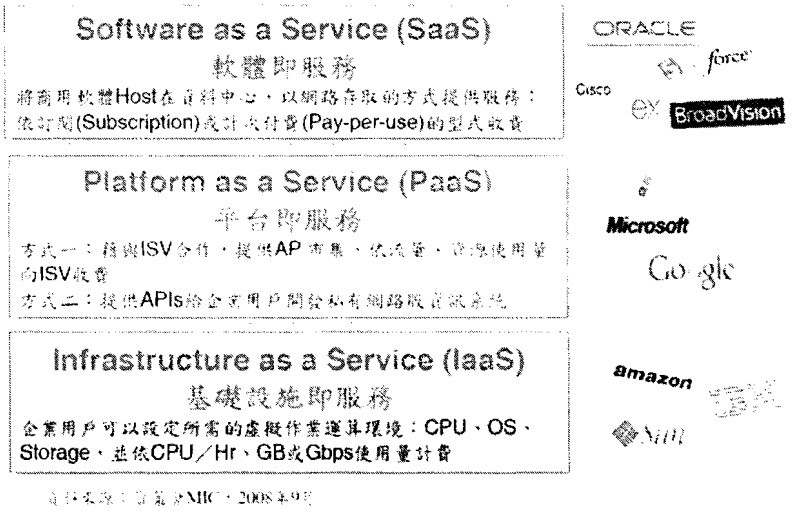

圖 2.2.1 雲端運算的三種架構

「基礎架構即服務」代表的是提供電腦硬體運算基礎設施，包括伺服器(Servers)、網路設施(Network Equipment)、記憶體(RAM)及儲存硬體(Disk)、CPU、資料中心設施等等。甚至在基礎安全方面如物理安全防護，周邊防火牆, 負載平衡，可能還有網路 IDS/IPS 等等，及相當的必須防護措施。

「平台服務」指的是基礎設施，ASP(Application Service Provider)服務供應商的雲端運算版，負責提供各項雲端服務。對於伺服器運算資源、網路頻寬、儲存設備的配置， 企業可依照本身需求使用電腦計算能力及空間需求的多寡支付月租費，省卻自行建置與購置的成本，降低自建的潛在營運風險及系統營運的維護成本。

「軟體服務」是指各類應用軟體架在平台服務上，利用網路連線多台電腦的運算工作，或是透過網路連線使用由遠端主機提供的服務。只要上網就可使用，使用者不需再下載至自己電腦，增加負擔。

舉例來說，一般民眾使用的電腦或手機，不需要安裝軟體，使用雲端軟體服務，連上網路就可以使用視訊，收發電子郵件，看全世界的電視節目（如衛星電視）等各種應用服務；對軟體程式設計師來說，可以利用既有廠商的平台來開發軟體，不需要投資在設備上，可以專注於程式開發。至於一般的中小企業，一開始不需要投資建置非常昂貴且技術門檻較高的資料中心，只要租用資料中心的服務，就可以在網際網路（Internet）專注開發與使用應用軟體服務，非常適合我國中小企業之發展環境。

2.3、雲端運算的服務模式

如果從雲端運算服務提供者與服務使用者的角度，雲端運算的服務模式可以分爲公有雲（Public Cloud）、私有雲（Private Cloud）、混合雲（Hybrid Cloud）3 類(如

圖 2.3.1 所示)。

所謂的公有雲就是由許多不同的使用者，共同分享雲端服務提供者所提供的雲端環境；私有雲則爲一個完整的雲端環境只由一家公司或組織內的成員所使用；而混合雲顧名思義就是公有雲與私有雲混合搭配使用。

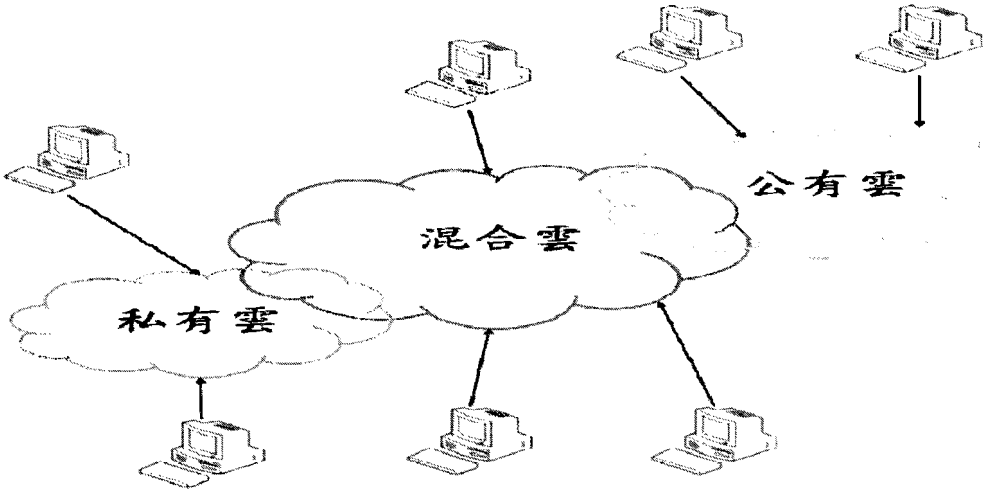

圖 2.3.1 雲端連算的三種服務模式

一般而言，小型企業就成本考量，以極少的經費就可以使用公有雲的服務；至於大型企業因爲已經擁有相當規模之 IT 基礎建設，在安全性的考量下，大多選擇適度調整目前 IT 架構轉換爲私有雲的架構。另外大型企業或政府機構也可以選擇混合雲的架構，基本上就是將一些對安全性與可靠性需求較低的應用，部署在公有雲架構上，可減少部分 IT 基礎建設之負擔，其他應用則仍是在私有雲架構下。

雲端運算比較特殊之處在於產業鏈的業者都可以直接提供服務給雲端運算的用戶，不一定存在價值鏈相依；換句話說，並非所有的雲端服務都必須同時提供上述三種類型的服務，例如亞馬遜（Amazon） 的 EC2 只提供客戶 IaaS 的服務，Google 的 GAE(Google Application Engine）專注於提供平台服務， 而 Salesforce.com 的客戶管理系統(CRM，Customer Relationship Management)則純粹是提供軟體服務。

各種雲端服務雖然眾說紛紜，但有三樣東西卻是它的必要組成，分別是：網路、運算、服務。換句話說，透過網路連線，由遠端所提供的強大運算和服務，讓企業可藉此改變以往的資訊處理方式，除了可提高作業效率，進而節省成本支出之外，同時更獲得資訊科技的創新應用。

2.4、雲端運算所帶來的利益

至於雲端運算究竟可爲企業帶來多少的好處，我們分別列舉以下幾點來說明：

2.4.1 擴充未來應用

雲端運算可讓企業快速部署及應用新科技，無論是應用服務的升級或擴展，在短時間之內就可完成，不必擔心資源耗費的問題。同時，服務的資源可以依據使用者的需求進行動態擴展和配置（On- demand Ser v i ces &Elasticity）。例如亞馬遜的 EC2 可以在短時間內提供使用者 200 台以上虛擬伺服器的資源，並在 3 至 4 小時任務完成後，快速回收資源並提供給其他用戶使用。

2.4.2 減少費用負擔

使用者依照需求使用雲端運算的服務，然後按實際使用次數、使用量，或是使用時間付費。有些公司必須購置大型 IT 設備與資源，以因應業務尖峰需求，但在業務淡季時，公司仍然必須維護大型資訊系統，以致許多資源閒置。若能運用雲端架構，企業平時不必維護多餘設備與資源，但可以在業務尖峰或因應突然之需求時，委由雲端運算服務提供者執行。

2.4.3 降低 IT 維護人員、減少營運成本

企業不需要再花錢去購買軟體和硬體，也不需要太多的資訊人員來開發或維運所需的應用服務，只需透過租賃硬體，軟體則採用使用者付費方式，大幅節省不必要的成本支出。

2.4.4 提供最新功能

雲端服務可以用客製化的方式提供給使用者使用，（Resource Pooling）。例如亞馬遜的 EC2 將運算處理能力包裝爲一種資源，並以服務的方式提供給用戶。此特性有助於平台或應用程式的更新，企業不需要不斷的花費時間或金錢來更新應用程式或軟體，同時藉由網路的連結來讓企業使用者的平台、應用程式及軟體達到一致性的客製化服務。

2.4.5 提高工作效率

隨著網路無所不在的連結性，無論工作者身在何處都可享有相同便捷的應用服務，而且藉由雲端強大的運算能力，可有效解決工作端運算效能不足的問題。且不論服務的資源實際來自一個地點或分散在多個不同地點， 最後都彙集成單一、整體的方式供使用者在任何地點運用（Ubiquitous NetworkAccess）。例如 Google 在全世界有上萬台伺服器，一般使用者在使用 gmail 或 youtube 服務時，實際的資料可能存在一台伺服器上，或分散儲存在不同的伺服器甚至不同地域的伺服器上，但對使用者而言沒有任何差異。

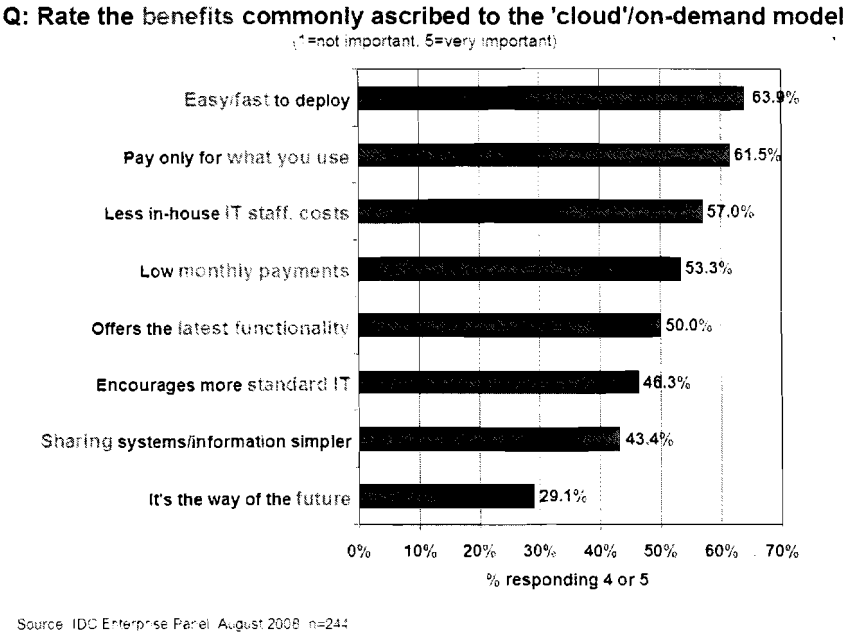

圖 2.4.1 雲端運算最吸引人的特性

參、雲端運算的資安風險

根據市場調查機構 Gartner 的研究顯示，未來以雲端運算方式所提供的安全應用服務，將會對市場造成相當大的衝擊，預估在 2013 年會比目前再成長三倍。而趨勢科技的調查則指出，雖然業界看好雲端運算在資安上的應用，但是也有 61% 的企業受訪者表示，除非可以確定應用雲端運算不會產生重大的資安風險，否則目前仍不會急於導入雲端運算的相關應用服務。

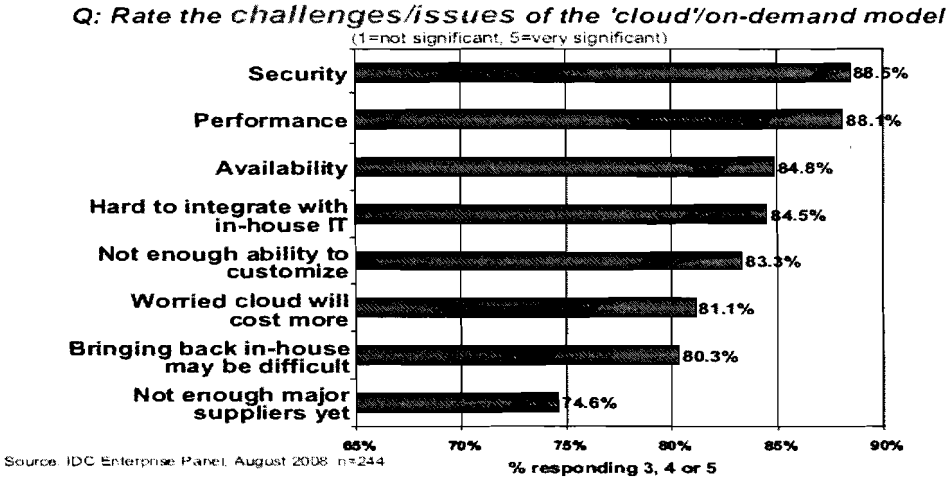

圖 3.1 導入雲端運算的困難點

3.1 目前面臨之問題

3.1.1 取得資料和資料分析將會變得非常簡單：

在雲端運算的崛起創造了巨大的資料庫和貨幣化的應用。例如：谷歌利用其雲端基礎設施來收集和分析消費者的廣告網路資料。即使是公司缺乏谷歌的資源，收集和分析資料都可能變得非常便宜。大量的資料和便宜的資料探勘會對隱私造成什麼影響？由於雲端的運用，攻擊者可能擁有龐大的，且密集的資料庫可供分析，也是用原始計算能力去取得這些資料庫。

3.1.2 敏感資料的隱藏：

我們注意到，隱藏資料是一個難題。例如，某醫院的資料庫已取消部分隱藏。工具是需要有效的隱藏，這將增加雲端中散發和收集更多的資料的重要性，需要進行安全分析或共享。一個例子間接表示資料探勘可能由一個雲端提供商關注交易和雙方的關係資料。例如，兩公司可能合併的議程正在審議之中時，被分享出去。

3.1.3 防護成本的有效性和可用性：

可用性還需要把攻擊者列在考慮範圍內，其目標只是爲了破壞活動。越來越多攻擊者因爲現實的政治衝突而走到了網路上。該損害賠償不僅關係到生產力的損失，而且其影響會延伸到雙方對於基礎設備的信任感問題，當此問題產生時，雲端用戶可能需要準備高昂的費用來進行資料備份。因此，必須制定方法的持續可用性。

3.1.4 客戶授權的安全問題：

典型用戶模式不必擔心任何行動會造成風險，他們由雲端執行安全管理，雲端維持軟體的運作。這種架構刺激用戶的流動性，但增加了需要解決認證安全的方式。此外，該動作對存取資料和應用程序增加，在雲端和較少依賴於特定用戶的機器很可能會增加網路釣魚和其它濫用技術來竊取密鑰的威脅，他們可能以其他方式獲得，例如，使用暴力攻擊方法。

3.1.5 混和模式的授權：

由於採用雲端運算的增長，我們有可能看到更多的服務執行混搭工具的資料。這方面的發展潛力及安全問題，無論是在資料洩漏條件，並在數量方面的資料來源，用戶可能要搜尋資料。反過來，要求如何獲得授權的可用性的原因：雖然集中查詢控制可以解決，但眾多的問題，要執行起來是非常困難且不恰當的。

從資訊安全的觀點來看，企業在運用新的資訊技術時，對於其隱含的資安風險，當然要做審慎的評估，而個人認爲在採用雲端運算服務方面，至少有三個層面需要考量。

首先是網路層面，因爲一旦商業運作需要仰賴雲端來進行，那麼網路頻寬的消耗，是否真如業者所言來的那麼節省？會不會拖累了原有網路服務的正常使用？這些都需要實地測試才可得知。另外，網路連線的穩定性也會比以往要求來

的更高，因此在網路管理方面，原有的網路設備是否需要擴充？如何進行網路效能的最佳化調校？網路備援的方式？這些可能都會變成隱藏的成本支出。而網路傳輸的安全性當然也要涵蓋其中，若是有敏感資料需要傳輸，那麼是否有相對安全的加密機制和身分認證機制等，都是使用雲端服務時必需的要求。

其次是資料層面，企業要放置什麼資料在雲端上，將會決定所需的安全強度，在採用雲端資料服務的初期，建議企業先以非敏感性的資料爲主，藉此來測試評估服務的安全性，而非一開始即將最重要的商業資訊，透過雲端方式來進行運算或儲存，以避免當資訊外洩時可能造成的衝擊。

最後是法規層面，企業要注意雲端服務廠商本身的安全是否值得信賴，是否有可供辨識的安全保證，例如取得政府的許可或國際標準 ISO 27001 的認證，因爲這代表了雲端服務廠商在資料保護、實體安全、應用程式安全、系統可用性、漏洞管理、法規遵循方面是否有一套完善的管理制度，對於資訊安全可提供一定的保障。另外，萬一不幸發生資安問題，在責任歸屬與賠償機制上，就有賴於事先的合約或服務等級協議(SLA)，所以在一開始的服務簽定時，企業法務部門的參與協助也是十分重要。

肆、雲端運算的技術解決方案

4.1、使用雲端運算的企業個案

雲端運算的技術正在起飛的階段，但技術的完整性仍是各大企業所必須傷透腦筋的，我們就以下幾項觀點及數個案例來說明：

4.1.1 採用雲端服務後，該如何考量安全層級？

雲端運算的安全性是企業最頭痛的問題，因爲雲端技術的架構，雖然虛擬化技術可以把硬體的使用率提升到最高，但這並不代表軟體的技術是完全安全的，同時，企業仍然關注那一種的安全層級才可達到企業的安全要求、針對各家的雲端服務商該如何選擇。以下我們將舉一個案例來說明企業使用雲端服務後，對於使用者的習慣可採用哪些技術來因應，同時說明該考量哪些要點。

案例一：幾個月前，有一家擁有 1,500 位員工的醫療器材公司的網路系統總監，委任 Lincoln Cannon 協助行銷部門轉換到 Google Apps，以及執行一個以 SaaS 爲基礎的教育訓練應用，這個計畫稱爲 eLeap，目的是降低企業的發展成本與增進生產效率。然而，採用雲端後所衍生的問題是行銷部門的主管不想採用超過一種的登入方式，而 IT 部門想維持原本的存取控制應用程式，尤其是當新員工加入，或員工離職時可以關閉帳號。

爲了解決網路系統總監所遇到的問題，Cannon 採取了以下的解決方案：

一、透過單一身份驗證與 AD 系統聯合運作

Cannon 改採用 Symplified 的單一登入系統，此系統可以和 Active Directory 互通，並可以同時確認登入雲端應用的使用者身份。Google Apps 利用 API 卸載用戶的身份驗證，再傳輸到單一登入供應商的端點，但是如果要用運用到 eLeap，系統必須使用一個驗證轉換器。

Cannon 表示：「要將 Google Apps 設置成 eLeap 的教育訓練，你必須利用單一登入供應商來進行身份驗證」，它同時與 Active Directory 一起運作。透過 Symplified，我們可以定義哪一個帳戶可以存取哪些應用程式，還有何時刪除在 Active Directory 中的帳戶；這一點可以預防任何人利用帳戶存取那些 SaaS 的應用程式。

二、PaaS：可彈性增加安全層級

在 SaaS 服務中，用戶不需要管理與控制基礎架構-網路、伺服器、操作系統或儲存設備，但是能控制他們所建置的整體應用程式，可能還有應用程式代管的環境組態設定。

PaaS 的在戶在整備或內建的安全功能上，這一點比 SaaS 來得少，加拿大標準協會 (Canadian Standards Association, CSA)那些功能的確較不完整，但是如果要增加額外的安全層級時則更有彈性。也就是說，除了使用者圍繞在應用程式介面(API)管珀安全問題(例如：驗證、授權與稽核等)之外，還必須花更多心思在應用安全上。

三、IaaS：資料加密與虛擬化的安全考量

CSA 對 IaaS 架構的解釋是用戶不但可以自己供應程式、儲存、網路與其他基本的運算資源，也可以建置、運作系統與應用程式。他們無法管理與控制底層的雲端基礎架構，但是他們可以控制整個操作系統、儲存與部署的應用，可能還有部分的網路組件控制權，像是主機防火牆。

四、內建安全功能不多，但擴充性大

據 CSA 解釋，在 IaaS 的服務架柿中除了保護基礎架構本身的安全之外，被整合進來的安全能力並不多，但是擴充性卻非常的大。這意謂著使用者必須透過 API 去管理及保護作業系統、應用程式及資料安全。

Kivas 表示：「很多的週邊防火牆是由供應商掌控，但是他們還是給你虛擬機器的存取權，因此你必須建立應用程式，並且提供基礎架構控制」。

五、確保不同用戶的切割

至於 IaaS，Heiser 認爲虛擬化的管理是一個很大的問題，尤其是入侵偵測及虛擬機器分割時的完整性部份。同時，供應商在虛擬化時，必須調節分割，並且確保它們不會交互影響。

Wescorp 的 CIO，Chris Barber 表示，他比較在意的是多租戶架構與管理程序的弱點問題。既然有很多個用戶在一個實體的機器上，就有可能會有安全上的弱點，

使用者可能會透過某種方式，存取其他用戶的虛擬機器。

4.1.2 雲端運算所使用的的技術，在私有雲的環境中如何最佳化？

雲端運算被視爲未來幾年內最大的商機，雲端運算的業者不斷的推動雲端服務，可是各大企業仍未必採用，原因在於各大企業並不了解雲端的各種技術，同樣的，各大企業也無因爲不了解技術，目前的大多數企業多是建置私有雲端服務，在有建置私有雲端服務的企業中，多數的企業會完全把私有雲的技術提升至 100%虛擬化，再考慮使用公有雲端服務或混合雲端服務，至於該如何建置 100%虛擬化的企業雲端服務呢？本文在此舉一個案例來說明：

案例二：Matt Reidy 是 SnagAJob.com 的營運總監，開始進行爲期三年的技術更新。他的目標是將公司已經進行虛擬化 75%的環境，完成 100%的虛擬化，以建立私有安全雲端運算，其技術核心採用 Dell 刀鋒伺服器運作 VMware 與 vSphere 虛擬化技術。以一個快速成長、充滿創意的商業網站而言，SnagAJob 需要的是一個彈性化的雲端運算架構，Reidy 表示：「我們尚未準備好採用其他供應商所提供的雲端服務。當許多事項開始運作時，我們所做的準備很有可能會半途中止，而虛擬的雲端基礎架構可以讓這些事，以最少的人力投資進行，只要花時間讓新項目快速啓動即可」。

爲了讓 SnagAJob 能完全的虛擬化，Reidy 採取了以下二個動作：

一、採用虛擬防火牆

技術更新之前，SnagAJob 有一個多層次(multitier)基礎架構，其防火牆將網路、應用程式與資料層進行實體分離。透過淘汰實體防火牆，以及建置 Altor Nerworks 的虛擬防火牆方式，完成了 100%的虛擬化。現在 SnagAJob 除了入侵偵測系統及防禦裝置外，唯一繼續存在的只剩最外層的防火牆了。

二、Vmsafe 的 API 介面提升了網路效能

Reidy 說：「在採用 vSphere 的第四版之前，你可以讓防火牆設像虛擬機器一樣的運作，但是，其效能受到嚴格的限制，因爲網路流量必須通過那些虛擬機器」，但是現在 vSphere 包含了稱爲 Vmsafe 的 API，它可以讓防火牆供應商，像 Altor、Checkpoint 等，把流量檢查移到 Vmware 的核心去進行。

Reidy 表示：「當採用了以上二種技術後，讓效能、穩定性與安全性等，提高了十倍」。有了 Altor 的虛擬防火牆，Reidy 的團隊可以同時看到，哪一種流量正在哪一台虛擬機器中流動，其中也包含了通訊協定與資料量。因爲 Reidy 的團隊可以看得見流量，所以可以更強固他們的安全，同時以它爲基礎，來思考相對應的規則制定。

4.1.3 儲存在雲端的資料及備份，該如何加密？

雲端運算的主要傳輸媒介是網際網路，網際網路的普及率加速了雲端運算的發展，而企業對儲存在雲端運算的資料或備份，難免會有敏感性資料，這使得企業對於雲端資料中心的安全性考量變得嚴格，同時，在雲端服務上的儲存位置，企業可做哪些考量呢？以下我們用案例來說明：

案例三：Allen Brewer 是紐約 Flushing 銀行的 CIO，Allen Brewer 在受夠了用磁帶備份後，開始採用雲端運算進行資料備份。他採用的是 Zecurion 公司的 Zserver 服務。現在 Flushing 銀行透過網路傳送檔案以儲存 備份。對這個銀行來說，最大的問題就是加密問題，還有，他們必須找到一個供應商，所提供的解決方案是可以使用目前所有的加密演算法。Allen Brewer 說：「我們一部份仰賴供應商的加密服務，但同時我們自己也進行自己的加密。」，「我們寄發的所有資料，與儲存在雲端供應商端的所有的東西都是被加密的」。

有幾個雲端所使用的備份儲存供應商，都是將裝置安裝在客戶端，來解決加密問題，但是 Flushing 銀行對這種安排不感興趣。Brewer 同時也選擇了 Zecurion 公司，因爲他可以知道自己的資料是儲存在哪一個資料中心，且能知道資料中心設置在哪裡。Brewer 說：「至少我們知道 Zecurion 的三個資料中心的其中一個，有我們的資料。採用雲端服務來備份資料，不是只有把資料上傳，而不知道自己的資料放在哪裡！」

4.1.4 採用雲端運算後，如何管理稽核問題?

雲端運算的虛擬化技術，使得硬體可以發揮接近 100%的使用率，也就是一台雲端主機可以服務多個用戶，這時會有新的問題產生，多個用戶同時在同一台主機上，而用戶該如何稽核或管理其他使用者在自己主機上的資料使用權呢？以下的案例可得知，當企業遇到人員的稽核的問題時，可以採行的解決方案：

案例四：Kavis 選擇了 Amazon 來代管整個基礎架構。在導入之前，他與一個安全專家仔細的研商過，安全專家確認部署虛擬機所需的所有設備。之前 Kavis 有建立一個可應用於控制部份功能的虛擬影像，並且開發一個快照功能，讓 Kavis 可以在需要的時候，隨時可以複製，爲得是快速的建立一個虛擬機器。

Kavis 也必需要執行系統管理者都能執行的所有功能，像是開啓或關閉連接埠、組態設定與鎖定資料庫等，這部份 Kavis 是使用 Amazon 的 LAMP 功能套件來完成。Kavis 非常滿意 Amazon 所提供的邊界安全，Kavis 說：「那是少數公司可以做到的等級」。

Kavis 也有考量到備份的問題，爲了確保營運不中斷，Kavis 將資料複到至少兩個不同的區域，Kavis 說：「唯一會把我擊潰的方法，就是 Amazon 的多重區域也崩潰了。」、「因爲 Amazon 的每個區域，其可靠性都很高，所以我們的備份不可能在同一時間、同時瓦解。」

最讓 Kavis 頭痛的問題是：如何應付人員稽核的問題？Kavis 說：「因爲雲端運算的稽核規則尚未明朗，管理規章仍要求必須到實體設備去處理，但你無法在公

有雲端這樣做。」，因此，Kavis 的計畫是採用私有雲端服務。Kavis 說：「如果你問供應商稽核方面的問題，供應商會說：『這是你的伺服器，請分別獨立做管理，如果他要做稽核，也請把要稽核的人員帶到獨立空間裡稽核』，我們目前是採用此種方法來稽核，可是我們其餘的資料都還是在公有雲端裡面」。

4.2、評估企業整體的應用安全

事實上，雲端運算服務除了造福企業之外，對於惡意的駭客而言，也算是一大福音，因爲這代表了許多企業更加依賴網路連線，會將重要的資訊透過網路傳輸，並且將商業資料儲存在企業環境之外，如果輕忽了可能的資安風險，就等於增加了駭客入侵的機會。

舉例來說，像是駭客可以利用雲端運算的強大能力來破解使用者帳號、密碼，竊取雲端所儲存的資訊；或是發動分散式阻斷網路攻擊(DDOS)，癱瘓雲端網路的運作，也就間接導致重要營運服務的停擺。另外，雲端資安服務機制的有效性，是否一如業者宣稱的可有效攔阻惡意程式入侵，是否會有潛藏的安全漏洞反而受到利用等，這些也都是未來需要關注的地方。

所以，企業在評估導入雲端運算的服務時，建議一開始先從非關鍵性的應用服務開始，而除了尋找可靠的雲端服務供應商之外，也要考慮有沒有其他的替代選擇。否則一旦企業所倚賴的雲端服務受到攻擊而停擺之後，將會對企業造成重大衝擊，例如：關鍵資料無法存取、客戶資料外洩、防毒系統失效、惡意程式入侵等等，這些都有賴於事前整體的考量，絕非像是購置單一硬體和軟體一樣，只要輕鬆以對即可完成。

對於資安廠商而言，除了銷售傳統的資安軟硬體設備，若是還能藉由雲端運算的協助加持，提供更多的資安加值應用服務，那是再好也不過了。根據我們的觀察，目前資安廠商運用雲端運算來提供的資安服務，大致有下列幾種：

一、病毒防護

讓防毒軟體的使用者，能夠即時回傳電腦上可疑的病毒相關資訊，就能在防毒業者的雲端上比對病毒特徵，不需要再等到防毒軟體更新病毒碼，就可有效防止病毒的感染。

二、網址過濾

面對日益增加的惡意網站，可協助企業透過雲端進行網址黑名單的比對，透過即時更新的惡意網頁資料庫，可以提高攔截的效率。

三、郵件過濾

配合傳統的垃圾郵件過濾機制，比對垃圾郵件如來源 IP、信件標頭等資訊，同時也可結合防毒功能，即時掃瞄郵件的附件是否安全。

四、身分識別

企業可透過雲端進行使用者身分認證，作到單一登入功能，讓使用者可在任何地點登入使用各項應用服務，解決使用者的授權問題。

伍、結論

雲端運算是目前在 IT 及各學術報告當中，是最流行的概念，各產業針對其資訊應用較明智的設計及發展，就是將他們的下一代系統部署到雲端運算。雖然許多對於雲端的預測可能是炒作，但雲端運算所提供的服務及企業的利益是不會改變的。無論是潛在客戶或是雲端用戶，推動雲端運算的最主要方法，就是消除客戶對於雲端運算的恐懼。爲了解決各大企業在導入雲端運算時所遭遇的問題，及其所採取的措施，這些措施應能解除使用者對雲端運算的疑慮，同時，參與雲端能顯著的提高商業智能及提升競爭優勢。

參考文獻

[1] P. Mell and T. Grance, "Draft nist working definition of cloud computing - v15," 21. Aug 2009.

[2] J. Napper and P. Bientinesi, "Can cloud computing reach the top500? " in Combined Workshops on UnConventional High Performance Computing Workshop plus Momory Access Workshop, 2009, pp. 17-20.

[3] Y. Chen, V. Paxson, and R. Katz, "What's New About Cloud Computing Security? ", 2010.

[4] A. Leinwand, "The Hidden Cost of the Cloud: Bandwidth Charges," http://gigaom.com/2009/07/17/the-hidden-cost-of-the-cloud-bandwidthcharges/,2009.

[5] M. Nelson, "Building an Open Cloud," Science, vol. 324, p. 1656, 2009.

[6] B. Sotomayor, R. Montero, I. Llorente, and I. Foster, "Virtual Infrastructure Management in Private and Hybrid Clouds," IEEE Internet Computing, vol. 13, pp. 14-22, 2009.

[7] T. Harmer, P. Wright, C. Cunningham, and R. Perrott, "Provider-Independent Use of the Cloud," in The 15th International European Conference on Parallel and Distributed Computing, 2009, p. 465.

[8] "Unified Cloud Interface Project,"http://code.google.com/p/unifiedcloud/.

[9] "Sun Microsystems Unveils Open Cloud Platform,"http://www.sun.com/aboutsun/pr/2009-03/sunflash.20090318.2.xml,2009.

[10] M. Zeller, R. Grossman, C. Lingenfelder, M. Berthold, E. Marcade, R.Pechter, M. Hoskins, and R. Holada, "Open standards and cloud computing: KDD-2009 panel report," in KDD, Paris, France, 2009, pp.11-18.

[11] L.Chia-Hwa, H.Shih-Kai," The Data Protection Scheme for Cloud Service", Proc. of the 2010 Conference on Computer Vision, Image Processing and Information Technology, Zhongli, Jun. 9, 2010

[12] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong," The Characteristics of Cloud Computing", in the 39th International Conference on Parallel Processing Workshops, 2010

[13] Fangzhe Chang, Jennifer Ren, Ramesh Viswanathan," Optimal Resource Allocation in Clouds", IEEE 3rd International Conference on Cloud Computing,2010

[14] Nils Gruschka and Luigi Lo Iacono," Vulnerable Cloud:SOAP Message Security Validation Revisited", IEEE International Conference on Web Services,2009

[15] Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito," How to Enhance Cloud Architectures to Enable Cross-Federation", IEEE 3rd International Conference on Cloud Computing,2010