以模糊函數建構動態安全風險管理模式 提升雲端運算環境的安全性

王淑卿　　江茂綸*　　嚴國慶*　　王順生*　　蔡思豪
朝陽科技大學
{scwang; mlchiang; kqyan; sswang; s9914603}@cyut.edu.tw
*聯絡人

摘要

在現今資訊發達的時代裡,網際網路已經成為使用者生活上不可或缺的媒介，更因為使用者希望獲得低成本但具有多元化的服務，因此雲端運算(Cloud Computing)迅速的竄起。而由於雲端運算的特性，使得現今企業在網際網路上提供的服務越來越多元化，也使得雲端環境的使用者快速的增加，改變了現有的商業模式。然而，在雲端運算環境中的服務系統與雲端應用服務必須面對可能遭到的威脅與風險，以致無法進行安全的配置。因此，本研究提出以模糊函數建構動態安全風險管理模式(Fuzzy-based Dynamic Security Risk Management model；FDSRM)，利用模糊理論的隸屬函數來進行服務系統與雲端應用服務的安全分析。而為了能減少系統資源的浪費，因此在本研究中，FDSRM 採用動態系統安全模型的層級，依據服務需求不同的安全等級需求，彈性的設定安全架構與安全機制，使雲端運算環境中的資源能夠有效的分配與使用，以提升雲端運算環境的安全性。

關鍵詞：雲端運算、模糊理論、隸屬函數、安全架構、安全機制

1. 前言

在現今資訊發達的時代裡，網際網路已經成為使用者生活上不可或缺的媒介，無論是購物、通訊、或繳稅…等，都可以利用網際網路去完成，使得使用者越來越依賴網際網路，也因為如此便利的技術，讓使用者對於網際網路有更多的服務需求。而為了提供更多且更方便的服務給予使用者，服務供應商必須能夠應付龐大的服務需求以及資料流量，所以服務供應商需要擁有足夠能力的伺服器。而傳統的網路服務供應商為提供更快更好的服務，則需增加伺服器的數量或提升伺服器的能力來應付新的服務或需求。因此，為了因應龐大的服務需求及資料流量，分散式系統(Distribute System)架構應運而生[7]。分散式系統的概念是將一個龐大的工作分割成數個子工作，再將各個子工作分配到不同的電腦進行處理。

在分散式系統的概念中，網格運算(Grid Computing)及 P2P(Peer to Peer)為其中最常被應用於在網際網路上[7]。然而，由於網際網路的蓬勃發展、電腦硬體的快速成長及網際網路頻寬的增加，使得現在的網路服務更加多元化，而網路的使用者也日漸增加，以使用者為導向的雲端運算(Cloud Computing)概念因應而生。而因為雲端運算有別於其他運算環境的特性，使得現今企業在網路上的服務越來越多元化，也使得雲端環境的使用者快速的增加，改變了現有的商業模式，能夠將目前已蓬勃發展的電子商務演變成以雲端環境為主的新型態模式[3,5]。

雲端運算是一種分散式運算的概念，「雲」即為網際網路；「端」則是指使用者端(Client)或泛指使用者運用網路來完成服務。換言之，雲端運算是一種新興的、極具延展能力的運算方式，能把資訊科技功能，包括運算、儲存及頻寬，以「服務」的形式，透過網際網路提供給網路的使用者[7]。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。雲端運算改變了傳統網路服務供應商的運作模式，創造了新型的服務方式，能夠把資訊科技的能力，包括運算能力、儲存能力以及頻寬速度，透過網際網路提供給使用者[1,3,4]。

由於雲端運算帶來的改變，目前在網際網路上所充斥著的服務，大部分都是使用雲端運算的技術來提供使用者更好的使用環境，例如 Google 的電子信箱、Dropbox 的儲存空間、Facebook 的交流空間、…等，甚至連網路遊戲都只需透過瀏覽器，無須下載任何應用程式就可以在網頁上使用。換言之，只要使用者利用設備連上網際網路，就可以使用雲端運算伺服器的服務及能力，且在雲端運算上的服務皆具有可攜性這樣的特性。亦即，在任何一部設備使用雲端運算的服務，都可以在另一部設備上繼續未完成的工作。

而且，由於在雲端運算的環境中，也可以利用協同工作的方式多人處理同一件工作。因此，伴隨著資訊科技及網路技術快速的發展，以使用者為導向的雲端運算，逐漸地成為各企業所矚目的焦點，所以把現今的「雲端運算」當作為「網際網路」的代名詞也不為過。

傳統的網際網路服務的型態為每一家服務供應商都擁有自己的伺服器，若是要服務更多的使用者則必須提升伺服器的能力或增加伺服器的數量，但當使用者的數目未達一定的程度時，則會浪費未使用的資源，以致造成企業成本的浪費。雲端運算利用了虛擬化(Virtualization)的技術來提供服務，將整個伺服器或個人電腦的資源虛擬成一個資源池(Pool)，可以依照服務的需求或服務的種類來提供資源，並且可以結合工作排程(Job Schedule)的方式，來降低系統資源的浪費，達到快速回應以及減少等待時間的特性[6,10]。

雲端運算為網際網路帶來更便利、更快速的環境，但在雲端運算的環境中存在著不同於傳統網際網路的安全風險，且當企業或使用者將重要的資料存放在雲端運算的環境中時，安全問題是必須被考慮的重要議題。在雲端運算環境中，不僅必須考慮安全問題，還必須要符合雲端運算環境架構上的特性。對於雲端運算環境的安全區隔，必須依照 TCP/IP 的層級被分為幾個安全區塊。除此之外，因服務需求的不同，所以對安全等級的需求亦不盡相同。因此，在雲端運算環境中必須以動態且具有彈性的機制來為不同的服務需求制定不同的安全等級，以符合每一個服務或需求之安全需求。如此，將可避免因為要確保服務或需求一定的安全程度，而對系統帶來過於龐大的負擔。因此，本研究是以符合雲端運算特性的安全機制做為探討的主題。

為符合雲端運算環境的安全需求特性，本研究提出以模糊函數建構動態安全風險管理模式(Fuzzy-based Dynamic Security Risk Management model；FDSRM)，可動態彈性的調整雲端服務需求之安全機制，以符合各項服務與需求的安全等級，來提供相對應的安全需求。換言之，透過 FDSRM 的使用，讓雲端服務提供者可調整更符合該服務或需求所需的安全等級。

本文第 2 節為文獻探討，探討雲端運算現有的安全模型以及安全層級；第 3 節說明本研究所提出的 FDSRM；第 4 節將探討本研究所提出的方法並分析；最後一節為結論與未來工作。

2. 文獻探討

在本節中將探討雲端運算所需的資訊安全要求、在雲端運算環境的風險與威脅分析、以及動態系統安全模型。

2.1 資訊安全需求

在雲端運算的環境中大致可分為三個層級，分別為網路層(Network Level)、主機層 (Host Level) 、及應用層 (Application Level)，在每一個層級對於資訊安全的要求各有不同[1]。詳細敘述將在以下章節說明。

2.1.1 保密性

在保密的要求上，要確保存放在雲端運算環境中的使用者之資料不會被未經授權的一方給存取。為達此目的，可以利用適當的加密技術來進行。除考慮加密的類型是對稱式或非對稱式的加密演算法外，金鑰的長度與金鑰的管理都是需考慮的因子。

至於採用那種加密技術，則由雲端服務供應商決定，如 MozyEnterprise 就有使用加密技術來保護顧客的資料，但是 AmazonS3 就沒有提供加密技術。除此之外，雲端服務供應商必須利用 NIST (National Institute of Standards and Technology，美國國家標準與技術局)的標準正確的部署加密的標準，才能確保使用者的資訊之高安全性。

2.1.2 完整性

在雲端運算的環境中，雲端的使用者不僅要擔心資料儲存或傳輸的安全性，資料的完整性也是必須被考慮的重要因素。由於在雲端運算環境中無法確保資料沒有被有心人士所篡改，因此資料可以透過加密的方式以確保其安全。為確保資料的完整性，主要的方法有兩種，一種是利用訊息認證代碼 (Message Authentication Code；MAC)；另一種為數位簽章(Digital Signature；DS)。

MAC 是將對稱式密鑰加入資料中，以提供一個校驗的碼。而 DS 的演算法，則是基於公開金鑰的架構。由於對稱式演算法的計算速度較非對稱式的演算法計算速度快許多，因此在對稱式演算法機制下，MAC 將會是提供完整的檢查機制較好的解決方法。由許多研究資料中得知，在雲端運算的 PaaS (Platform as a Service)與 SaaS (Software as a Service)中是不提供任何資料完整性的保護，因此在雲端運算的環境確保資料的完整性是非常重要的

2.1.3 可用性

在雲端運算環境中，當已授權的使用者要求資料時，除了必須提供資料的完整性外，資料的可用性亦是必須考慮的重要因子。由於，被威脅的目標或資料的可用性很難驗證或保障。因此，為達成資料的可用性，可透過許多強而有力的技術，去預防與避免可用的服務或資料遭受威脅或影響，如分散式阻絕服務(Distributed Denial of Service；DDoS)攻擊或者雲端服務供應商的可用性等。

2.2 風險分析

風險分析有狹義和廣義兩種，狹義的風險分析是指通過定量分析的方法給予完成任務所需的費用、進度、性能三個隨機變數的可實現值的概率分佈。而廣義的風險分析則是一種識別和測算風險，開發、選擇和管理方案來解決這些風險的有組織的手段。

風險分析是對風險影響和後果進行評價和估量，包括定性分析和定量分析。其中，定性分析是評估已識別風險的影響和可能性的過程，按風險對項目目標可能的影響進行排序。其作用和目的為：識別具體風險和指導風險應對；根據各風險對項目目標的潛在影響對風險進行排序；通過比較風險值(Risk Scores)確定項目總體風險級別。定量分析是量化分析每一風險的概率及其對項目目標造成的後果，也分析項目總體風險的程度。其作用和目的為：測定實現某一特定項目目標的概率；通過量化各個風險對項目目標的影響程度，甄別出最需要關注的風險；識別現實的和可實現的成本、進度及範圍目標。

因此，在雲端運算環境中進行的風險分析，即為管理檢查所有已經確認的弱點，其最大的效益就是確認雲端服務的提供是否謹慎的進行。而在雲端運算環境中所需進行的風險分析，包括威脅分析及弱點分析。

2.2.1 威脅分析

在安全的威脅部份，是指惡意軟體(或有心人士)由遠程利用基礎設施的組件、網路服務以及應用程式的漏洞，對雲端服務造成影響，這是雲端服務一個主要的威脅。表 1 所示為在雲端運算環境中可能產生的威脅，包括：威脅來源、威脅產生的動機及其產生威脅的行為。

2.2.2 弱點分析

在進行雲端運算環境的風險分析時，可以透過弱點掃瞄提供各個主機上的弱點資訊，接著即可利用修補程式進行漏洞的修補工作。弱點分析是辨識系統漏洞的一個重要過程，能夠保護主機、網路設備與應用程式已知的漏洞不被攻擊。

目前針對弱點分析已有漏洞識別的過程，包含連接應用服務之網際網路常規的掃描系統，評估組織的弱點風險，最後並以修復過程來解決弱點分析的風險。表 2 所示為在雲端運算環境中可能產生的弱點，包括：弱點、弱點產生的來源及其產生威脅的行為。

表 1 威脅辨識

威脅來源	動機	威脅行為
駭客(Hacker) 鬼客(Cracker)	挑戰自我	系統入侵、未經授權系統訪問
電腦犯罪	資料銷毀、非法取得資訊、金錢利益、未經授權修改資料	電腦犯罪(例：Cyber Stalking)、詐欺行為(例：重送、模擬、截取)、資訊賄賂、欺騙、系統入侵
恐怖份子	勒索、銷毀、復仇	炸彈或恐怖主義、訊息戰、系統攻擊(例：Distributed Denial of Service)、系統滲透、竄改系統

表 2 弱點辨識

弱點	威脅來原	威脅行為
前員工系統帳號未從系統移除	前員工	進入公司的網路取的公司專有的資料
公司防火牆允許遠端登入與利用來賓帳號執行某服務	未經授權用戶(例：黑客、被解雇的員工、電腦罪犯、恐怖分子)	利用來賓帳戶來遠端登入到某服務進行系統檔案的瀏覽
系統供應商已發現設計上的漏洞，且新的更新還未被更新至系統	未經授權用戶(例：黑客、被解雇的員工、電腦罪犯、恐怖分子)	根據已知的系統漏洞，未經授權的存取敏感的系統文件

2.3 動態安全模型

圖 1 所示是由 Yildiz 等人[12]所提出的動態安全模型架構，這個模型包含四個層級，分別為網路層(Network)、儲存層(Storage)、服務層(Server)及應用層(Application)。企業依據其需求(Enterprise Security Principles)在這四個不同的層級上，分別制訂其安全的高低等級。而在這四個層次上的安全等級的決定則是動態依據系統管理的要求(Dynamic System Management Security)。

垂直為特定的層級的端點到端點的安全強度，例如，儲存層的水平安全政策只包含對相關的安全物件進行儲存的政策。垂直設計為覆蓋各個層級的端點口，例如，一些安全物件可能介於服務層與儲存層，也可能有部分屬於每一層。垂直動態

的政策可確保公共物件或任何例外都包含在安全模型內。

基於每一層的水平政策，該層級的安全要素，可由最低到最高的安全政策來做配置。例如，可依據安全物件所需要的安全等級來做分為等級一至等級十，越敏感或越需要安全的等級則設定越高。

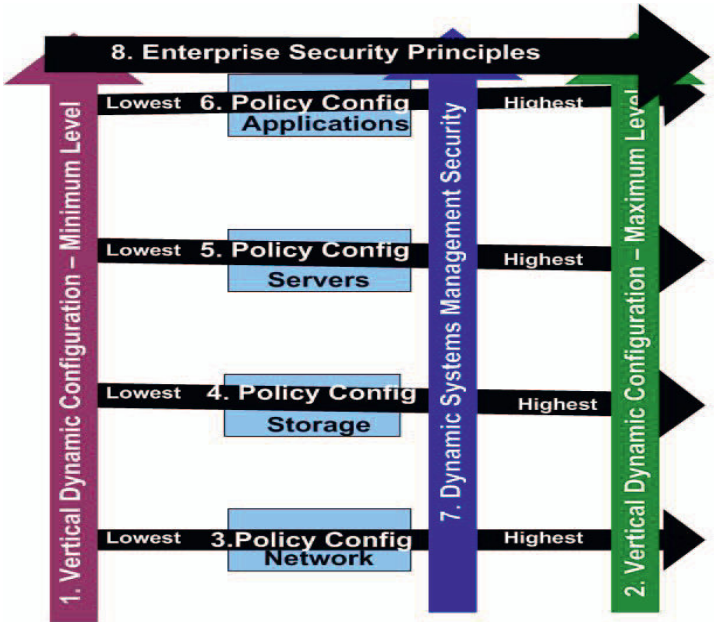

圖 1 動態系統安全模型

3.研究方法

由於雲端運算的特性，使得現今企業在網路上提供的服務越來越多元化，大量的雲端服務供應商匯聚成雲端市集，改變了現有的商業模式。而因為雲端運算環境中擁有大量的雲端服務供應商，使得雲端使用者在這共用的雲端市集上，尋求適當的服務。然而，目前在雲端運算環境中所提供的雲端服務，其服務的需求大多未透過安全的機制來進行保護。因此，雲端使用者在這樣的環境下無法確保需求是否已被竊聽或竄改。

為了解決雲端運算環境的安全性，有些研究將過去使用在分散式系統的安全機制使用在雲端運算環境上。然而使用這些安全機制，其作法是在將服務送到伺服端時必須經過重重複雜的程序才能保障服務需求的安全，但是在雲端運算環境中其服務需求非常的大量，因此對於系統整體是一個很大的負擔，以致無法滿足快速且安全的服務環境給使用者。

因此目前各個雲端服務的提供者，在雲端運算環境中提供多元化的雲端運算服務的同時，也使用各式各樣的安全技術或安全機制。然而在雲端運算這個共享的環境中，所使用的安全機制或安全技術，都必須符合該服務與環境的需求。而在現今的雲端運算環境中，同一個服務供應商所使用的安全機制與安全技術，大部份都是藉由相同的方法來進行不同服務的安全措施。因此，本研究將在雲端運算的環境中建置一個較彈性且可符合各個不同服務類別的安全需求之模型架構，並藉由彈性的安全機制來提高各項服務的安全性與降低資源的消耗。

在 Zhang 等人的研究中[14]，提出以安全係數做為風險管理與威脅管理的一個參考值，但是在雲端運算的環境當中，該架構所計算出的安全係數無法符合雲端運算環境下的彈性需求。本研究所提出的方法稱之為以模糊函數建構動態安全風險管理

模式(Fuzzy-based Dynamic Security Risk Management model；FDSRM)。

FDSRM 利用 Yildiz 等人[12]所提出的動態系統安全模型作為基底，將雲端運算分為網路層(Network)、儲存層(Storage)、服務層(Server)及應用層(Application)四個層級，並且利用 Zhang 等人[14]所提出的安全係數結合模糊理論(Fuzzy Theory)中的隸屬函數(Membership Function)來設計符合雲端運算環境的彈性安全機制，藉以提高雲端運算環境中的安全性。在以下各節中將分別說明安全係數結合隸屬函數的設計，以及威脅程度的計算。

3.1 隸屬函數設計

本研究所設計的隸屬函數，包含兩個部分，分別是威脅及風險數量的隸屬函數，以及依據各服務供應商所注重的威脅與風險的隸屬函數。首先制定風險及威脅數量的隸屬函數，評估多少數量的風險及威脅會開始有成長的趨勢，到多少數量會呈現都是 1 的水平線。接著，再利用所注重的威脅與風險的隸屬函數來分別制訂服務或系統所遭受的威脅及風險，並給予相呼應的隸屬函數。最後，再將所得到的兩個隸屬函數作計算，就可以取得該威脅或風險占整個服務或系統的安全係數。

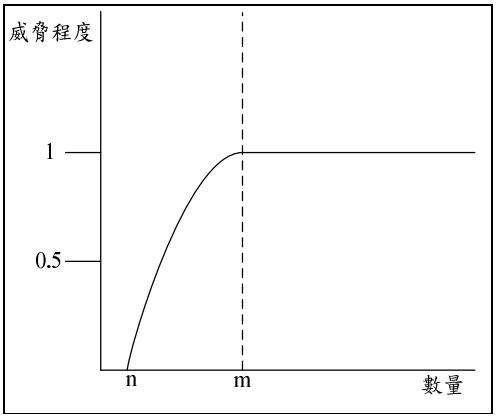

圖 2 威脅與風險數量(較不嚴重)

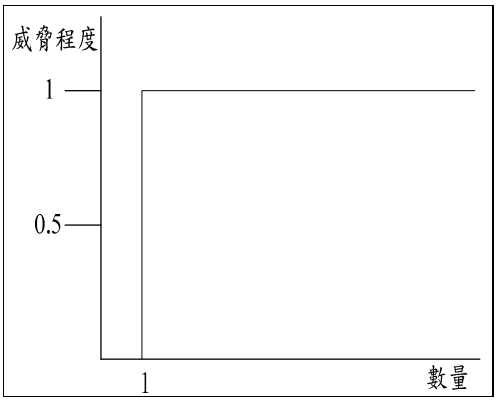

圖 3 威脅與風險數量(嚴重)

圖 2 與圖 3 分別表示威脅與風險數量的隸屬函數。圖 2 為較不嚴重的威脅與風險，*n* 值為起始值，可以設為 0 就開始有隸屬函數。例如，數量 10 開始為 0.1，每增加 10 個數量就成長 0.1，當值到達 100 個數量之後威脅程度就會到達 1，之後要是超過 100 個數量之後都是 1。也可以設定數量 10 為 0，然後每增加 5 個數量就增加 0.1，依此類推的方式，來做設定。除此之外，亦可以直接設定 *m* 值，往回推算隸屬函數。圖 3 則表示為較嚴重的威脅與風險，若是該威脅或風險 1 個就可能會造成系統或服務當機或者是無法提供服務的嚴重性，則設定為 1 個的隸屬函數為 1。

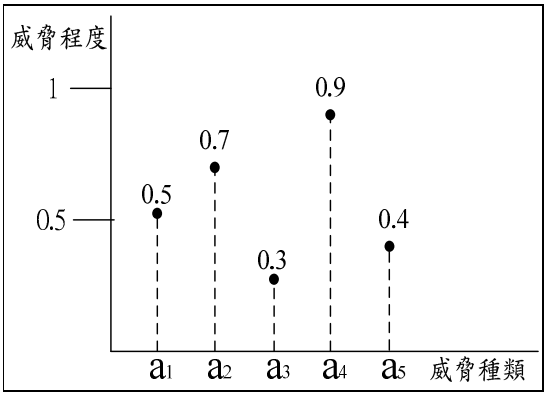

圖 4 威脅與風險種類

圖 4 所示為威脅與風險的種類，a_1 到 a_5 都是依據該供應商的系統或服務所遭遇到的威脅與風險，並且依照該威脅或風險對於系統或服務的威脅程度給予相對應的隸屬函數。例如，一個提供儲存服務的服務供應商，其所遭遇的威脅或風險可能就

存在著資料被竄改與竊取、資料的備份或者是資料的可用性...等。因此，給予每一個威脅與風險一個隸屬函數後，最後再與該威脅或風險所存在的數量做計算，就可以算出該威脅或風險在系統或服務的威脅程度是多少，然後再依照威脅程度給予相對應的安全機制與安全程度。

3.2 威脅程度計算

若是只有取得威脅數量以及威脅種類的隸屬函數，只能判斷出該威脅或風險對於系統造成的傷害程度。因此，若是僅僅依照該隸屬函數設置安全機制或安全技術，就可能會造成資源浪費的情況，因為有些威脅或風險對整個系統或服務是個很嚴重的問題，而有些威脅或風險只是輕微的威脅，但卻因為威脅的數量龐大而給予相對應的安全機制或安全技術，或許只需要利用較簡單的安全機制或安全技術則可以解決該威脅或風險。所以，接著需要計算該威脅或風險對於整個系統或服務的威脅程度與比例，然後就可以依照威脅的程度與比例來分配相對應的資源做安全的配置。

計算威脅程度的包括：該威脅或風險在系統所占的比例及該威脅或風險在整個威脅或風險中所占的比例等兩類，公式(1)所計算的 $T(x)$即為該威脅或風險在系統所占的比例及該威脅，公式(2)所計算的 $P(x)$即為該威脅或風險在整個威脅或風險中所占的比例。

$$T(x)=((A(x)+N(x))/2)/M$$
$$P(x)= T(x)/(T(1)+ T(2)+\ldots+ T(M))$$

其中，

$A(x)$： 威脅或風險的隸屬函數。

$N(x)$：該威脅或風險的數量隸屬函數。

M： 為威脅與風險的總數。

威脅程度計算的步驟如下：

步驟 1：	設定威脅與風險數量的隸屬函數。
步驟 2：	設定威脅與風險種類的隸屬函數。
步驟 3：	以 $T(x)=((A(x)+N(x))/2)/M$，來計算該威脅與風險在系統或服務所占的比例。
步驟 4：	帶入 $P(x)= T(x)/(T(1)+ T(2)+\ldots+ T(M))$，取得該威脅或風險在整個威脅與風險所占的比例。

經由計算之後，可以由 $T(x)$的總數相加得知整個系統或服務有多少比例是遭受威脅或風險，依照算出的數值從而改進系統或服務的安全機制，再依照 $P(x)$所計算出的比例，分配資源做安全機制或安全技術的設置。

整體而言，因此，本研究所提出的以模糊函數建構動態安全風險管理模式(Fuzzy-based Dynamic Security Risk Management model；FDSRM)，首先利用模糊理論的隸屬函數來進行服務系統與雲端應用服務的安全分析。在進行安全分析時，分別針對威脅與風險數量、威脅與風險種類，分別判斷各威脅或風險對於系統造成的傷害程度。接著，計算各威脅的程度，包括該威脅或風險在系統所占的比例及該威脅或風險在整個威脅或風險中所占的比例，然後再依照威脅程度給予相對應的安全機制與安全程度。最後，採用動態系統安全模型的層級，依據服務需求不同的安全等級需求，彈性的設定安全架構與安全機制，使雲端運算環境中的資源能夠有效的分配與使用，以提升雲端運算環境的安全性。本研究所提出的以模糊函數建構動態安全風險管理模式，如圖 5 所示。

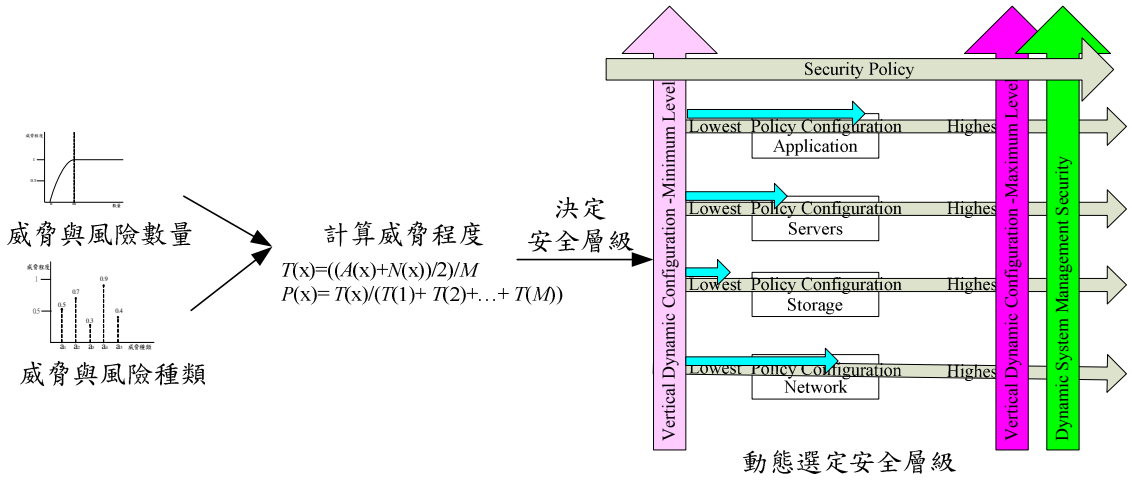

圖 5 以模糊函數建構動態安全風險管理模式

4. 方法分析

為提供雲端運算環境中一個安全無虞安全機制，過去已有學者提出設置安全機制的架構或分類與權重值，但這些安全機制無法提供雲端運算環境中所需要的彈性要素。因此，本研究提出 FDSRM，透過模糊理論的隸屬函數，針對雲端服務可能發生的威脅與風險之數量與種類進行運算，讓雲端運算環境中所需的安全機制與安全技術，能夠彈性的配置，藉以減少資源的浪費。透過 FDSRM 運算後，可以得知該系統或服務中存在著多少比例的威脅，進而改進系統或服務的安全品質，提升雲端運算的安全性。以下以三個部分，針對本研究所提出的 FDSRM 來進行分析。

4.1 安全性

在本研究所提出的 FDSRM，運用了模糊理論隸屬函數的方法對整個系統或服務進行安全性的分析。FDSRM 利用模糊理論的隸屬函數對雲端服務可能發生的威脅與風險進行威脅程度的分析，然後將隸屬函數的值帶入算式，進行整個系統與服務的威脅與風險的分析。接著，則可以利用分析後的結果，分別對弱點來做安全的配置。同時，利用 FDSRM 分析後的值得知系統或服務整體的安全概況，也可以經由過去所遭受到的攻擊或者未來可能會遭受到的攻擊，對在雲端運算環境中的系統與服務進一步的驗證其安全的需求。

除此之外，FDSRM 也可以搭配動態系統安全模型來對整個雲端運算架構進行分層的動作，並依照每層層級的需求以及已經遭遇或未來可能遭遇的威脅與風險進行分析，對雲端運算的架構做較佳安全配置。

4.2 資源負載

過去有關網際網路安全架構的建置，大都是依照該服務最注重的安全因子來進行安全的配置，而當發現其它的漏洞時，才會去做下一步的安全配置，因此往往沒有顧慮到資源的消耗。而本研究所提出的 FDSRM，搭配動態系統安全模型來做整體架構的安全分析，並從中可依照分析的結果來調整安全之配置。且，由於在雲端運算的環境中所提供的服務眾多，因此使用者所提出的需求量會非常的龐大，而經由 FDSRM 進行安全分析後，可利用結果對安全的配置進行資源平衡的動作，來減少資源的浪費，亦不會對雲端服務的品質造成影響。

4.3 彈性架構

在本研究所提出的 FDSRM 中，除了可以依照分析結果對整個系統或服務來進行安全的威脅與風險之檢測，更可以配合動態系統安全模型來分析整個雲端運算的架構。除此之外，並可以依照模型的每層層級進行安全的調整，不會因為要提高系統與服務安全性，而去加強每個層級的安全機制或安全技術，以致提高服務供應商的成本與增加資源的浪費，更可能會進一步影響到使用者的服務品質。所以，以本研究所提出的 FDSRM 進行安全的分析，可依據雲端服務供應商所注重的安全因子以及必須顧慮到的安全需求來進行彈性的安全配置。

5. 結論與未來研究

在現代資訊快速發展以及硬體設備價格低廉的情況下，大量低價格的個人電腦漸漸取代了伺服器，結集成現今的雲端運算。由於雲端運算的出現，改變了現今的商業經營模式並且帶來了新的商機與新的營運模式。由於進入雲端運算環境的門檻極低，已有許多企業紛紛投入了雲端運算的環境，以降低企業所需的營運成本。而為擴展更多使用者群，許多企業在雲端運算的環境中，投入了多樣化及便利的雲端服務，也因此使得現今在雲端運算環境中有著各式各樣的雲端服務。

然而，當企業將更多的網路服務應用放在雲端運算環境中時，促使在網際網路的服務應用的數量與種類急遽增加。而因為在雲端運算的環境中存在著大量的服務應用，因此不得不考慮這些雲端服務的安全架構之配置與機制。

在現今針對網際網路的系統與服務所提出的安全模型與架構，雖然可針對服務應用的某方面之安全進行分析與設置，但是若將其運用在雲端運算環境中將缺少彈性的特性。除此之外，若將現有的安全模型與架構應用在雲端運算的環境中，則可能會造成無謂的資源浪費，降低雲端服務的服務品質，所以本研究提出了一個符合雲端運算特性的彈性安全架構，將可以加強雲端運算中系統與服務的安全需求。

本研究依據雲端運算的特性，提出 FDSRM，以提供雲端運算環境中系統與應用服務的彈性安全架構。除此之外，更結合動態系統安全模型將整個雲端運算架構分成不同的層級，然後再依各層級所需的安全機制或技術來進行安全的配置。因此，除了可遵循 FDSRM 分析的結果來進行資源的分配，減少在安全架構上的資源浪費，並可提升雲端運算環境的安全性。

因為雲端運算是一個較新的分散式系統之概念，因此若在雲端運算環境中使用傳統網際網路的安全機制，除了運算成本不能不加以探討外，雲端運算環境所需的彈性安全機制也是傳統網際網路的安全機制無法解決的議題。所以在未來的研究中，將針對雲端運算中的安全架構，依照各方面的需求來進行安全機制的配置，藉此可以提供更加穩定且安全的雲端運算環境給使用者與服務供應商，並且依照彈性的特性來做安全架構的基礎，來保留雲端運算的特性。

致謝

這篇論文是國科會計畫(NSC97-2221-E-324-007-MY3)研究成果的一部份，我們在此感謝國科會經費支持這個計畫的研究。

參考文獻

[1] S.A. Almulla and Y.Y. Chan, “Cloud Computing Security Management,” *Proceedings of the 2nd International Conference on Engineering Systems Management and Its Applications (ICESMA2010)*, Sharjah, 2010, pp. 1-7.

[2] A. Chonka, J. Singh, W.L. Zhou, “Chaos Theory Based Detection against Network Mimicking DDoS Attacks,” *IEEE Communications Letters*, Vol. 13, No. 9, 2009, pp. 717-719.

[3] N. Gruschka and M. Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services," *Proceedings of The IEEE 3th International Conference on Cloud Computing, Miami*, 2010, pp. 276-279.

[4] M. Jensen, J. Schwenk, N. Gruschka, and L.L. Iacono, "On Technical Security Issues in Cloud Computing," *Proceedings of The CLOUD IEEE International Conference on Cloud Computing, Bangalore*, 2009, pp. 109-116.

[5] L.M. Kaufman, "Data Security in the World of Cloud Computing," *IEEE Security & Privacy*, Vol. 7, No. 4, 2009, pp. 61-64.

[6] Y. Luo, "Network I/O Virtualization for Cloud Computing," *IT Professional*, Vol. 12, No. 5, 2010, pp. 36-41.

[7] B.P. Rimal, E. Choi, and I. Lumb, "A Taxonomy and Survey of Cloud Computing," *Proceedings of The NCM2009 5th International Joint Conference on INC, IMS and IDC*, Seoul, 2009, pp. 44-51.

[8] S. Ramgovind, M.M. Eloff, and E. Smith, "The Management of Security in Cloud Computing," *Proceedings of The 2010 Information Security for South Africa (ISSA)*, 2010, pp. 1-7.

[9] W.G. Tzeng, *Data Confidentiality and Robustness in Decentralized Cloud Storage Systems*, Dissertation of National Chiao-Tung University, 2010.

[10] G. Wang and T.S.E. Ng, "The Impact of Virtualization on Network Performance of Amazon EC2 Data Center," *Proceedings of The 29th IEEE Conference on Computer Communications* (IEEE INFOCOM), San Diego, 2010, pp. 1-9.

[11] L.C. Wang, K. Ren, W.J. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," *IEEE Network*, Vol. 24, No. 4, 2010, pp. 19-24.

[12] M. Yildiz, J. Abawajy, T. Ercan, and A. Bernoth, "A Layered Security Approach for Cloud Computing Infrastructure," *Proceedings of 10th International Symposium on Pervasive System, Algorithms, and Networks*, Kaohsiung, 2009, pp. 763-767.

[13] H.W. Zhao and R.X. Liu, "A Scheme to Improve Security of SSL," *Proceedings of the Pacifi-Asia Conference on Circuits, Communications and Systmes (PACCS)*, Chengdu, 2009, pp. 401-404.

[14] X. Zhang, N.T.P. Wuwong, H. Li, and X.J. Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments," *Proceedings of the 10th IEEE International Conference on Computer and Information Technology*, 2010, pp. 1328-1334.