Commerce & Management Quarterly, Vol.14, No.2, pp.143~164 (2013)

企業導入雲端服務專案之風險評估

RISK ASSESSMENT OF CLOUD SERVICES PROJECT FOR ENTERPRISES

王平
崑山科技大學資訊管理系副教授
柯文長*
崑山科技大學資訊管理系助理教授
蕭雅文
崑山科技大學資訊管理系研究生

Ping Wang
Associate Professor, Department of Information Management
Kun Shan University

Wen-Chang Ko
Assistant Professor, Department of Information Management
Kun Shan University

Ya-Wen Shiau
Graduate school student, Department of Information Management
Kun Shan University

摘要

雲端運算給資訊科技產業帶來商機，但亦帶來重大的挑戰。客戶願意採用雲端服務的前題是須確保客戶資訊安全。近期發生的網路進階持續性滲透攻擊（advanced persistent threat，APT）已導致客戶對導入雲端服務產生心理障礙。針對導入雲端服務所面臨的潛在風險問題，本研究提出一套風險評估方法，參考雲端安全聯盟（cloud security alliance，CSA）與歐洲網路與資訊安全局（European network and information security agency，ENISA）所提出的雲端服務之資訊安全架構，已決定導入雲端服務

*通訊作者，地址：710 台南市永康區大灣路 949 號，電話：06-2051630
Email：wcko@mail.ksu.edu.tw

之風險項目，利用模糊層級分析法（fuzzy analytic hierarchy process，FAHP）合理評估與分析雲端服務之風險項目優先順序。所研提的方法與案例分析，有助於企業了解轉移應用程式至雲端服務的風險項目及控管優先順序，以利決定資安資源分配及降低系統導入後之潛在衝擊。

關鍵字：風險評估、雲端運算、模糊集合、模糊層級分析法

ABSTRACT

Cloud computing presents the IT industry not only with exciting opportunities, but also with significant challenges since consumers are reluctant to adopt cloud computing solutions in the absence of firm guarantees regarding the security of their information. Network attacks such as APT attacks present a serious obstacle to consumer acceptance of cloud service project nowadays. Accordingly, the present study proposes a project risk assessment scheme and constructs a risk evaluation matrix based on the security framework followed by both Cloud Security Alliance (CSA) and European Network and Information Security Agency (ENISA). In addition, the risk priorities of attributes are rationally evaluated by fuzzy analytic hierarchy process (FAHP) method in the risk assessment process. Overall, the results confirm that the proposed method provides an effective means of recognizing the risk attributes and their risk priorities, deciding the allocation of risk budget, and reducing the impact of potential risk for enterprises.

Keywords: Risk Assessment, Cloud Computing, Fuzzy Sets, Fuzzy Analytic Hierarchy Process (FAHP)

壹、緒論

競爭力是企業在市場上必備的條件，雲端運算（cloud computing）服務已被企業所重視。隨著資訊系統的發達，雲端服務也跟著蓬勃發展，近來已成為網路上最熱門的議題之一。雲端運算是一個電腦與網路技術整體運用的新概念，不是一項全新的技術，而是分散式運算（distributed computing）與網格運算的新服務模式。雲端運算允許讓不同服務在一台主機上同時處理，提升資訊處理之效率並降低使用與

維護成本。然而，雲端服務（cloud services）也面臨著許多潛在的風險問題，企業在於執行導入雲端服務專案中，不易察覺與掌控雲端服務之資訊安全風險，恐將無法安心的導入雲端服務。為提昇企業掌控雲端服務之資訊安全風險的能力，降低雲端資安事件所帶來的潛在風險，本研究利用模糊層級分析法（fuzzy analytic hierarchy process，FAHP）提出一套專案風險評估方法，以利企業在導入雲端服務專案時進行風險評估，協助了解雲端服務之風險項目與其優先順序，以利未來之風險監控與資源控管。

資訊安全之風險管理已經逐漸受到重視，國際標準組織（international organization for standardization，ISO）制定了與資訊安全相關的標準，以利企業擬定資訊安全需求，及進行風險評估及控管，以確保導入資訊服務之資訊安全。已有許多學者以決策分析的概念來評估屬性項目，但在雲端服務風險評估上，大都以防護機制之架構或以 ISO 27001 之 133 項控制項目作為雲端運算風險的綱要，以建構資訊安全稽核表，作為企業評估雲端服務之風險項目。目前歐盟組織與資安組織深入探討雲端服務之資訊安全風險，其中雲端安全聯盟（cloud security alliance，CSA）探討在雲端上關於當前和未來的最佳做法來確保雲端服務運作之安全，詳見“雲端安全聯盟（CSA）雲端運算之安全的最佳做法”（CSA, 2010）；而歐洲網路與資訊安全局（European network and information security agency，ENISA）公布的「雲端運算：利益、風險與資訊安全建議」（ENISA, 2010）；開放式網站應用程式安全計畫（Open Web Application Security Project，OWASP）於 2010 年統計並公佈 Web 應用的十大資安風險項目。

本研究依據雲端安全聯盟（CSA）與歐洲網路與資訊安全局（ENISA）提出的資訊安全架構，決定雲端服務之風險屬性項目。考慮在進行風險評估的過程中存在不確定性及具模糊的特性，採用模糊集合（fuzzy sets）（Zadeh, 1965）處理各項不確定因素，並結合層級分析法（analytic hierarchy process，AHP）（Saaty, 1980）方法，進行各項雲端服務之風險項目的優先順序評估，依據各項風險項目之權重高低加以運算，以決定其風險值。本研究結果不僅可以協助企業導入雲端服務之風險評估依據，進一步可做為企業導入雲端服務時修補資安漏洞及持續監控資安風險的參考。

本文共分為五節，各節內容簡述如後，第二節，首先針對專案風險管理、雲端服務與其資訊安全以及群體決策進行簡介以及文獻探討。第三節說明風險評估模式，介紹模式進行的步驟與評估方法，第四節，依據第三節所提出之方法進行雲端服務專案之風險分析，並針對分析結果進行相關的討論。最後，依據本研究之研究目的與研究結果提出簡潔的結論與指出未來研究。

貳、專案風險管理與雲端運算服務

本章節將介紹專案風險管理、雲端服務與其資訊安全以及多準則決策之文獻探討。

一、專案風險管理

依據美國專案管理協會（project management institute，PMI）（PMI, 2008）所出版“A Guide to the Project Management Body of Knowledge”定義，「專案」為開發一特定產品、服務或欲得到特定結果所進行所投入工作規劃與發展的階段性組織。任何的專案執行過程常會有一些意外的事件發生，導致原預定的目標無法達成。許多不確定性的因素在當初的專案計畫中以完善的規劃與納入管理，有時候還會有一些突發狀況以及不可預料的事件發生，將升高專案風險。為能使專案能夠順利達成目標，就需在事前儘可能排除以降低風險的威脅，故專案規劃時須落實風險管理，有系統的辨識、分析事件的危害性、嚴重性以及回應專案事件的過程稱為風險管理（risk management），它強調是在於發生風險事件前所採取行動，不是事後採取補救措施，專案風險管理已被認為是組織工作項目的重點。

ISO 於 1997 年參考 PMI 提出的專案管理知識體系（project management body of knowledg，PMBOK）為架構，提出專案管理品質指導綱要，即《ISO-10006 專案品質管理系統指南》並也成為《ISO 9000 品質管理系統指南》中重要之支援性技術指導綱要（管孟忠，2011）。專案風險管理包括規劃、識別、分析、回應與監控過程，其目的是為了減少對專案威脅事件發生的機率與衝擊。專案風險繼承了所有專案皆存在不確定性（uncertain），針對已知風險，管理人員須運用風險管理程序，並預估當發生威脅事件時所產生對專案的衝擊；針對未知風險，專案團隊須審慎的回應並做緊急應變計畫，降低對專案帶來的衝擊。

近期相關研究包括 Kutsch and Hall（2010）提出以專案風險管理的方式，針對風險性高的項目提供防護機制，進行有效的管理，並做優先順序建議。Chapman（2001）探討了進行鑑定和評估的過程中，所涉及的專案風險，其來源必須考量到環境、市場、供應商與專案的因素，分析各因素影響風險分析的相關性。Marques, Goure, and Lauras（2010）在產品和服務的發展專案決策分析，提出了一個新多維項目績效指標測量，協助專案人員對風險的管控。

二、雲端運算服務與其資訊安全

雲端運算服務可分為三種型態（IBM, 2009）。第一種為“軟體即服務”（software as a service，SaaS），SaaS 之應用軟體的管理和維護由服務供應商提供，使用者付費使用 SaaS 所提供的軟體。第二種為“平台即服務”（platform as a service，PaaS），PaaS 提供程式服務與雲端設備，使用者依據合約所規範的權限，可以自行修改所需的服務與程式碼，不須承擔管理軟硬體的責任。第三種為“基礎設施即服務”（infrastructure as a service，IaaS），IaaS 的服務是建立在虛擬機器上，提供開發環境給使用者使用，使用者只需依照使用量付費，即可在雲端使用各種軟硬體、伺服器以及資料儲存和網路設備等服務。企業在考慮導入雲端運算服務時，除了必須了解企業主要的目的、既有的資訊安全政策與作業程序，還須評估各種雲端運算服務之潛在風險。

企業運用雲端運算服務，或許可提升營運效率，但是在於安全的考量上也許隱含著許多問題，尤其是資訊安全、個人隱私以及確保企業營運服務不中斷等等。CSA（2010a）提出「雲端運算首要安全威脅」（top threats to cloud computing）的報告，舉出七大雲端安全威脅，包含(1)雲端運算被人濫用或惡意使用(2)不具安全的應用程式開發介面(3)不肖的內部人員(4)共用技術的問題(5)資料損失或外洩(6)挾持帳戶或服務 (7)其他風險因素－與他人共用雲端廠商資源、硬體、軟體版本與軟體更新的風險。ENISA 公布的「雲端運算：利益、風險與資訊安全建議」（ENISA, 2010），對企業運用雲端運算服務提出 24 項雲端風險項以及對運用雲端運算服務之安全措施提出三項建議：(1)在於雲端運算服務的兩端須建立信任機制(2)大型跨組織機構須執行電腦鑑識以及數位證據資料的保護措施(3)建立大型電腦系統工程的資源隔離機制、不同雲端運算服務平台之間之溝通及系統回復能力機制。考慮企業內部資訊需藉由雲端服務供應商所提供的管理機制進行資料存取及分析，劉家驊與洪士凱（2010）提出以架構導向雲端運算服務之資訊安全防護機制，在傳送企業內部重要資訊前，先以架構導向將資料依企業目標與任務做整體性的規劃與分類，分類不僅須與企業目標相互呼應，同時又可運用資料進行適當的整理以決定適當的資訊安全防護機制。

考慮 IaaS、PaaS 及 SaaS 等三種雲端運算服務型態，整體雲端運算服務的安全議題與傳統的資訊安全防護，尚未見有效的方案提供雲端運算服務在使用安全的保證。忽視資訊安全管理將可能造成企業營運資訊外洩，嚴重影響商譽，如何消除企業對於雲端運算服務的資訊安全疑慮，使企業對網路服務供應商的資訊安全管理產生信心，是導入雲端運算的重要事務。蔡一郎（2010）提出雲端生態系統的概念，

用偵測、預警及防禦這三種機制，建構自我防禦的架構，可讓雲端運算服務環境更具安全。鄭進興與陳堂昇（2010）運用雲端運算為基礎，提出以 ISO 27001 之 133 項控制項目建立雲端運算服務的資訊安全管理制度，以降低 CSA 所提出之雲端運算服務的七大安全威脅並且指出企業必須定期對員工進行資訊安全教育及訓練，促使員工瞭解資訊安全的重要性及各種可能的安全風險。王平、林文暉、郭溥村、王子夏與盧永翔（2010）針對 ENISA 及 CSA 所提資安議題，深入探討及建議防護措施，降低導入雲端運算服務所帶來的風險。分析 ENISA 所提出弱點及威脅，透過 ISO27001 資安控制項之檢核，分析威脅對資訊資產弱點的衝擊損害（impact loss），推理估算資訊資產之風險值。IBM 所提出「IBM 觀點：安全與雲端運算」（IBM, 2010）之雲端安全建議，是依據 IBM 研究團隊及客戶經驗將雲端安全措施分為 8 大類，25 項要點，以利企業的創新且同時能降低公司內部的安全複雜性。彭秀琴與張念慈（2010）說明目前行政院所屬各級機關約有 3,800 個，大小電腦機房約有 3,000 個，為了維持這些機房基礎架構的運作，佔據大部分的資訊經費，在面對資訊經費與人力逐年減少，導入雲端運算服務為解決困境的良方，進一步考量的資訊安全事項並建立評估的步驟。黃富祿、張力允、李仁鍾與周碩聰（2010）透過對 Thin Client 雲端運算探討，藉由德菲法（Delphi method）反覆與單位內資深專業人員完成導入考量因素資料彙整，並完成問卷製作及資料彙整，再透過 AHP 層級分析法分成三層的因素層級，取得評估指標各項權重後，運用決策樹迴歸法針對各權重做進一步分析，實驗結果得知各單位資訊系統管理人員在考量導入 Thin Client 系統架構時，主要以系統管控及資料安全防護的需求度為主要考量。上述的文獻可得知，近幾年資訊安全逐漸受到重視。

三、多準則決策在群體決策的應用

企業導入雲端運算服務專案時，存在許多不可避免的潛在風險，在進行群體決策來評估雲端運算服務專案風險時，每位決策者對於問題的看法與結果均有不同，彼此之間常常會發生衝突，這種衝突很可能是不同的價值觀、偏好或者溝通不良所造成。因此，能有效處理這些衝突之問題，就要使用多準則決策來做處理。Kuo, Wang, and Tien（2010）運用資料包絡分析（data envelopment analysis，DEA）和網路分析法（analytic network process，ANP）與多屬性決策分析（multi-attribute decision analysis，MADA）來評選綠色供應商。由於評估屬性時，大多數的訊息是主觀和不準確的，而模糊集理論提供了一個數學模式來表達不精確性和模糊性。Chuu（2009）在台灣自行車行業採用先進製造技術的評價以及模糊理論來分析多個屬性，讓結果更加客觀與公正。多屬性群體決策反映群體決策在於決策單中有一定程度上影響。Pang and Liang（2012）針對語言訊息的多屬性群體決策的結果作評價。Chauhan and Vaish（2012）

使用多屬性決策之方法來選擇磁性材料。上述的文獻可得知，有關於方案的評選之問題在管理科學領域中有許多研究成果，應用多準則決策在群體決策過程中，可避免決策者之間不同的價值觀、偏好或者溝通不良所造成的衝突且能達到一個更客觀且公正的結果。

參、專案風險評估模式

本研究以 FAHP 評估雲端服務專案之各項風險，在整合多屬性群體決策對各項風險評估指標之重要性意見的過程中，同時考慮到群體決策對各項風險評估指標的重要程度及優先順序存在主觀判斷的不確定性及模糊性，發展出一套專案組合的評價模式。

一、模糊集合理論

傳統集合，又稱為明確（crisp）集合，一個集合的論域為 X 中的某一元素 x，表達屬不屬於某一集合 A 的方式為完全屬於或是完全不屬於此集合 A，也就是所謂的對或錯、0 或 1 的明確劃分表達方式。Zadeh（1965）提出模糊集合（fuzzy sets）來處理模糊不確定的問題。人類在現實社會中，對於事物的認知、思維與推理，存在著許多模糊性，例如：有人提問，今天天氣如何？答案會因為每個人認為熱的程度而有所不同。模糊集合 $\tilde{A}$ 的定義為 $\tilde{A}=\{x,\mu_{\tilde{A}}(x)\mid x\in X\}$。其中，所有元素 x 屬於論域 X，$\mu_{\tilde{A}}(x)$稱為 x 在模糊集合 $\tilde{A}$ 的隸屬函數（membership function），$\mu_{\tilde{A}}(x)$的結果為隸屬程度（grade of membership）。

在模糊集合理論中，允許元素 x 與模糊集合 $\tilde{A}$ 之關係可以是介於「屬於」與「不屬於」之間的任何一種隸屬形態，隸屬於的程度可以是介於 0 到 1 之間的任何一個值，以隸屬函數表示其隸屬程度，$\mu_{\tilde{A}}(x)\in[0,1]$。利用歸屬函數定義模糊集合 $\tilde{A}$ 有助於了解任一元素隸屬於模糊集合 $\tilde{A}$ 的程度。一個模糊集合 $\tilde{A}$ 的 α-截集（α-cut）定義為：在論域 X 中，所有對模糊集合 $\tilde{A}$ 之隸屬度大於或等於 α 之元素所組成的集合。α-截集表達方式為 $\tilde{A}^{\alpha}=\{x\mid\tilde{A}(x)\geq\alpha\}$，α-截集也可以以隸屬函數型態表達，其表示式為 $\mu_{\tilde{A}}(x)=\{x\mid x\in X,\mu_{\tilde{A}}(x)\geq\alpha\}$。圖 1 為 $\tilde{A}$ 之 α -截集的示意圖，其中，$\tilde{A}^{\alpha}=[A^{L},A^{U}]$，其上界表示式為 $A^{L}=\inf_{x\in[0,1]}\{x\mid\mu_{\tilde{A}}(x)\geq\alpha\}$，下界表示式為 $A^{U}=\sup_{x\in[0,1]}\{x\mid\mu_{\tilde{A}}(x)\geq\alpha\}$。本研究以對稱式三角模糊數與非對稱三角模糊數來表示專家不同的偏好。

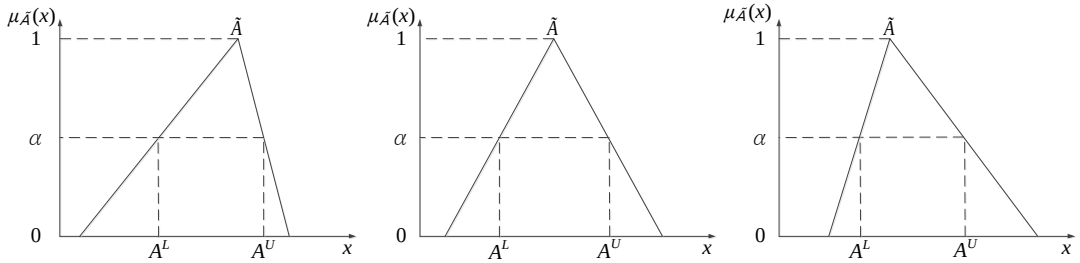

圖 1　$\tilde{A}$之 α-cut 示意圖

二、模糊層級分析法

傳統 AHP 可解決需要同時考慮量化與質化複雜的問題，同時採取多位決策者的意見，AHP 屬於多準則決策裡的多屬性決策方法（multi-attribute decision making，MADM），在一群可行方案，評估各屬性的相對重要性，決定方案的優先程度以及採取優先處理的順序。Saaty（1978）之傳統層級分析法因人類對於事物的認知、思維與推理具模糊性，因此有學者 Laarhoven and Pedrycz（1983）將它加以演化，發展出模糊層級分析法（fuzzy AHP，FAHP）。FAHP 是結合模糊數的觀念來處理評估準則之衡量與判斷等模糊不確定的問題。模糊層級分析法的執行步驟包含以下七個階段:(1)建立層級結構(2)三角模糊數的建立(3)模糊成對比較矩陣的建立(4)成對比較矩陣的模糊權重的計算(5)解模糊化(6)驗證一致性(7)整體層級權重計算與排序。

(一)層級結構的建立

蒐集各個學者與專家之風險評估相關文獻資料，探討雲端運算服務所牽涉到的風險屬性。完成風險評估架構的屬性後，再依據問題的複雜度加以檢視，各屬性之間是否具有獨立性，每一層的屬性盡量最好不多於七個項次。

(二)建立三角模糊數

傳統的 AHP 在於評估尺度中，以名目尺度來評估，並沒有考慮到人類語意的判斷具有模糊性，因此本研究選擇以語意模糊數來充分表達判斷的評估值，其中 AHP 屬性評估尺度使用五等級模糊名目量尺，代表評估者使用的語意量詞，例如以集合 S 來表示為 $S=\{I_1,I_3,I_5,I_7,I_9\}$，其 I_1 代表重要性非常低的衡量值，其餘 I_3、I_5、I_7、I_9 依此類推，如圖 2 所示；介於五個基本尺度之間衡量值為 I_2、I_4、I_6、I_8，如圖 3 所示。

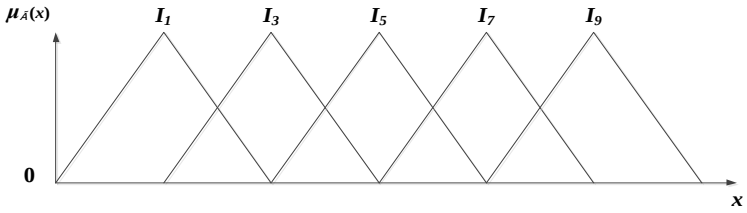

圖 2　評估尺度衡量值之三角模糊數隸屬函數圖

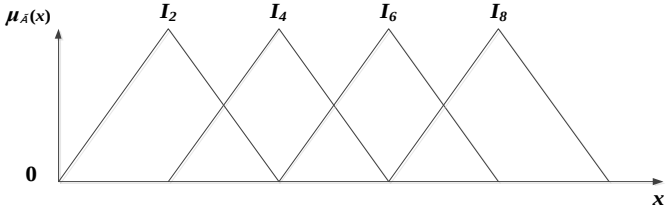

圖 3　評估尺度間之衡量值三角模糊數隸屬函數圖

(三)建立模糊成對比較矩陣

若有 n 個屬性時，進行成對比較之次數為 n（n-1）／2 次，進行成對比較時，所用的數值分別由模糊數來表示，比較完的結果的衡量，放入 $\tilde{X}$ 成對比較矩陣 n × n 的右三角裡，主對角線為各屬性自己與自己的相比值，因此皆為 1。左下三角裡，為右上三角的倒數，即 $\tilde{x}_{ij}=1 / \tilde{x}_{ij}$。表示式：

$$\tilde{X}=\begin{bmatrix} 1 & \tilde{x}_{12} & . & . & . & \tilde{x}_{1n} \\ 1/\tilde{x}_{12} & 1 & \tilde{x}_{23} & . & . & \tilde{x}_{2n} \\ . & 1/\tilde{x}_{23} & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 1/\tilde{x}_{1n} & 1/\tilde{x}_{2n} & . & . & . & 1 \end{bmatrix} \quad (1)$$

(四)計算成對比較矩陣的模糊權重

1.群體意見整合

本研究利用模糊幾何平均數整合專家意見，整合的運算式為：

$$(x_{ij})_{\alpha}=\left[\frac{1}{\sqrt[m]{\prod_{\zeta=1}^{m}\left(x_{ij}^{(\zeta)}\right)_{\alpha}^{L}}},\frac{1}{\sqrt[m]{\prod_{\zeta=1}^{m}\left(x_{ij}^{(\zeta)}\right)_{\alpha}^{U}}}\right] \quad (2)$$

其中，$(x_{ij})_{\alpha}$ 表示模糊成對比較矩陣中第 i 列第 j 行之 α *-cut* 的代表值，m 為專家數，ζ 為第幾個 α *-cut* 值，$\frac{1}{\sqrt[m]{\prod_{\zeta=1}^{m}\left(x_{ij}^{(\zeta)}\right)_{\alpha}^{L}}}$ 為上界值之模糊幾何平均數，$\frac{1}{\sqrt[m]{\prod_{\zeta=1}^{m}\left(x_{ij}^{(\zeta)}\right)_{\alpha}^{U}}}$ 為下界值之模糊幾何平均數。

2.計算模糊權重值

Saaty（1980）提出的四種方式來求得近似之權重值，分別為行向量平均值的標準化、列向量平均值的標準化、行向量和倒數的標準化以及列向量幾何平均值標準化等四種方式。而本研究利用列向量平均法來計算出模糊權重，此方法可得到模糊成對比較矩陣的模糊權重值，其表示式為：

$$\tilde{w}_i=\frac{\sum_{j=1}^{n}\tilde{x}_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{n}\tilde{x}_{ij}} \quad (3)$$

其中，$\tilde{w}_i$ 為矩陣中每一列之模糊權重值，n 為屬性個數。

(五)解模糊化

由於專家評估內容可能存在偏好不一致的問題，Saaty（1990）進一步提出一致性檢定地方法，以確認評估偏好具一致性的要求。然而，以模糊數表示的評估結果恐不易進行一致性檢定，因此，先進行解模糊的處理，以確保一致性檢定得以進行。本研究利用半線性解模糊化法（Semi linear defuzzification method，SLIDE）（Yager & Filev, 1993）做為模糊評估值 $\tilde{x}$ 之解模糊的工具，其方法提供了一個簡單而不複雜的解模糊過程。其表示式為：

$$d=\frac{(1-\lambda)\sum_{i\in L}u_i x_i+\sum_{i\in H}u_i x_i}{(1-\lambda)\sum_{i\in L}u_i+\sum_{i\in H}u_i} \quad (4)$$

其中，$L=\{(i\ /\ u_i) < y, i=[1,n]\}$與 $H=\{(i\ /\ u_i) < y, i=[1,n]\}$，依據 SLIDE 之方法以 α-cut 的方式來進行，其表示式為：

$$w=\frac{(1-\lambda)\sum\limits_{\substack{q\\ \alpha_q<y}}\alpha_q x'_{\alpha_q}+\sum\limits_{\substack{q\\ \alpha_q\geq y}}\alpha_q x'_{\alpha_q}}{(1-\lambda)\sum\limits_{\substack{q\\ \alpha_q<y}}\alpha_q+\sum\limits_{\substack{q\\ \alpha_q\geq y}}\alpha_q}\quad ，\lambda\in[0,1]，y\in[0,1]，q=1,\ldots,Q \qquad （5）$$

其中，Q 表示 α-cut 的數量，α_q 代表第 q 個 α-cut 之 α 值，本研究依據 Mabuchi（1993）所提出之概念，令代表第 q 個 α-cut 之 $\tilde{x}$ 的代表值。$x'_{\alpha_q}=0.5\times(x^L_{\alpha_q}+x^U_{\alpha_q})$

(六)一致性檢定

成對比較矩陣為一正倒數矩陣（positive reciprocal matrix），在這個部分要要求決策者能達到成對比較前後一致性，是相當困難的。依照上個步驟將群體整合後之模糊成對比較矩陣解模糊化之後，得到的值來做一致性的檢定。因此，運用一致性檢定來作為一致性指標。Saaty（1990）提出以一致性指標（consistence index，C.I.）與一致性比例（consistence ratio，C.R.）作為成對比較矩陣一致性的檢定。整個層級結構，一致性比例建議在 0.1 以下（Saaty, 1990）。

(七)整體層級權重計算與排序

依前述步驟可求得整體層級權重計算，其運算式為：

$$w'_j=w_i\times w_{ij} \qquad （6）$$

其中，w_i 為第一階層第 i 個主要屬性的權重，w_{ij} 為第一階層第 i 個主要屬性下第 j 個評估項目的權重，第二階層相對第一階層的第 i 項主要屬性之各項風險屬性的風險權重。

依照上述步驟先建立層級結構，接著建立每位專家的評估意見，各項評估值以三角模糊數，針對評估者所評估之結果建立模糊成對比較矩陣，依照多位評估者的模糊成對比較矩陣進而群體整合，將群體整合後之模糊成對比較矩陣內之三角模糊數，經解模糊化得到之結果驗證一致性並計算各屬性的模糊權重值，最後，求得整體層級權重，其結果將可進一步決定各項風險屬性的風險優先順序。

肆、專案風險評估案例

讓企業公司可有效永續經營，而在市場中具備競爭能力，本研究之案例為某公司導入雲端運算服務專案來作為說明雲端服務專案風險之評估範例。本案例是針對雲端運算服務為主，依據 ENISA（2010）所建議的雲端運算服務架構，考慮的風險屬性為 24 項。

(一)層級結構的建立

本研究依據 24 項風險屬性，建構雲端服務風險威脅之風險評估層級架構，第一階層考慮「政策及組織帶來的風險」、「技術風險」與「法律」三大類別，並且展開各類別之第二階層的風險評估項目（屬性），詳細的風險評估屬性如圖 4 所示。

(二)以三角模糊數評估風險項

本研究考慮多位專家參與風險評估，且每位專家對風險評估尺度具有不同的偏好。為克服風險評估尺度的不確定性本質，每位專家對於風險屬性之意見可採用不同的三角模糊數表示，以代表其個人對屬性之風險偏好（態度）。假設有五位對風險偏好（樂觀程度）不同的專家參與雲端運算服務風險的評估，每位專家對風險評估尺度之偏好，如表 1 所示。在表 1 中，每位專家的對不同的風險尺度都以（「下界值」，「最有可能值」，「上界值」）表示。

(三)建立模糊成對比較矩陣

依據圖 4 之雲端運算服務風險威脅層級架構，針對五位專家對於第一階層三大類別與各個類別下第二階層所屬屬性之意見採用不同的三角模糊數表示，以式(1)建立出五位專家針對第一階層三大類別「政策及組織帶來的風險」、「技術風險」與「法律」所構成的 3x3 模糊成對比較矩陣及第一類別「政策及組織帶來的風險」下第二階層之七個屬性所構成的 7x7 模糊成對比較矩陣、第二類別「技術風險」下第二階層之十三個屬性所構成的 13x13 模糊成對比較矩陣與第三類別「法律」下第二階層之四個屬性所構成的 4x4 模糊成對比較矩陣。並利用式(2)把上述五位專家所建立出的第一階層三大類別模糊成對比較矩陣與各個類別下第二階層所屬屬性之模糊成對比較矩陣，將模糊成對比較矩陣內的每個元素做群體之整合，整合過後的第一階層三大類別及各個類別下第二階層所屬屬性之模糊成對比較矩陣。以第一階層三大類別「政策及組織帶來的風險」、「技術風險」與「法律」所構成的 3x3 模糊成對比較矩陣為例，以 $\tilde{B}_1$ 表示整合五位專家意見的評估結果：

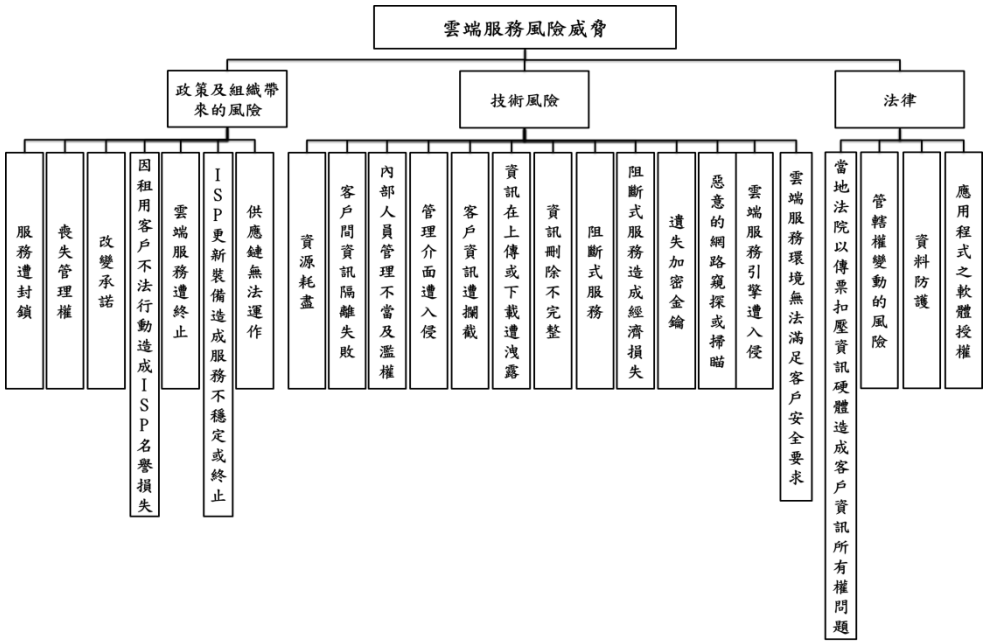

圖 4　雲端運算服務風險威脅之層級架構（ENSIA, 2010）

表 1　每位專家模糊語意之模糊數

尺度	語意描述	專家 A	專家 B	專家 C	專家 D	專家 E
I_1	非常低	（1, 1, 2）	（1, 1, 2.2）	（1, 1, 2.4）	（1, 1, 1.8）	（1, 1, 1.6）
I_2	介於兩者之間	（1, 2, 3）	（1.4, 2.2, 3.4）	（1.8, 2.4, 3.8）	（0.6, 1.8, 2.6）	（0.2, 1.6, 2.2）
I_3	低	（2, 3, 4）	（2.6, 3.4, 4.6）	（3.2, 3.8, 5.6）	（1.4, 2.6, 3.4）	（0.8, 2.2, 2.8）
I_4	介於兩者之間	（3, 4, 5）	（3.8, 4.6, 5.8）	（5, 5.6, 7）	（2.2, 3.4, 4.2）	（1.4, 2.8, 3.4）

續下表

續表 1

尺度	語意描述	專家 A	專家 B	專家 C	專家 D	專家 E
I_5	中等	(4, 5, 6)	(5, 5.8, 7)	(6.4, 7, 8.4)	(3, 4.2, 5)	(2, 3.4, 4)
I_6	介於兩者之間	(5, 6, 7)	(6.2, 7, 8.2)	(7.8, 8.4, 9.8)	(3.8 ,5, 5.8)	(2.6, 4, 4.6)
I_7	高	(6, 7, 8)	(7.4, 8.2, 9.4)	(9.2, 9.8, 11.2)	(4.6, 5.8, 6.6)	(3.2, 4.6, 5.2)
I_8	介於兩者之間	(7, 8, 9)	(8.6, 9.4, 10.6)	(10.6, 11.2, 12.6)	(5.4, 6.6, 7.4)	(3.8, 5.2, 5.8)
I_9	非常高	(8, 9, 9)	(9.8, 10.6, 10.6)	(12, 12.6, 12.6)	(6.2, 7.4, 7.4)	(4.4, 5.8, 5.8)

表 2　雲端運算服務之風險三大類別與各個類別所屬屬性之模糊權重值

類別	類別模糊權重值	屬性	屬性模糊權重值
政策及組織帶來的風險	(0.276, 0.292, 0.304)	服務遭封鎖	(0.180, 0.183, 0.184)
		喪失管理權	(0.100, 0.113, 0.120)
		改變承諾	(0.335, 0.320, 0.306)
		因租用客戶不法行動造成 ISP 名譽損失	(0.042, 0.034, 0.040)
		雲端服務遭終止	(0.230, 0.232, 0.229)
		ISP 更新裝備造成服務不穩定或終止	(0.035, 0.034, 0.032)
		供應鏈無法運作	(0.077, 0.084, 0.089)
技術風險	(0.129, 0.105, 0.1　00)	資源耗盡	(0.097, 0.097, 0.100)
		客戶間資訊隔離失敗	(0.166, 0.159, 0.154)
		內部人員管理不當及濫權	(0.163, 0.158, 0.151)
		管理介面遭入侵	(0.050, 0.052, 0.058)
		客戶資訊遭攔截	(0.048, 0.052, 0.056)
		資訊在上傳或下載遭洩露	(0.024, 0.023, 0.027)

續下表

續表 2

		資訊刪除不完整	（0.096, 0.097, 0.099）
		阻斷式服務	（0.022, 0.023, 0.025）
		阻斷式服務造成經濟損失	（0.015, 0.015, 0.015）
		遺失加密金鑰	（0.046, 0.052, 0.053）
		惡意的網路窺探或掃瞄	（0.017, 0.017, 0.018）
		雲端服務引擎遭入侵	（0.094, 0.097, 0.096）
		雲端服務環境無法滿足客戶安全要求	（0.162, 0.158, 0.148）
法律	（0.595, 0.604, 0.596）	當地法院以傳票扣壓資訊硬體造成客戶資訊所有權問題	（0.514, 0.505, 0.493）
		管轄權變動的風險	（0.286, 0.296, 0.301）
		資料防護	（0.135, 0.144, 0.153）
		應用程式之軟體授權	（0.065, 0.054, 0.053）

$$\tilde{B}_1 = \begin{bmatrix} (1,1,1) & (1.80,2.95,3.97) & (0.25,0.34,0.56) \\ (0.25,0.34,0.56) & (1,1,1) & (0.17,0.20,0.26) \\ (1.80,2.95,3.97) & (3.78,4.93,5.88) & (1,1,1) \end{bmatrix}$$

(四)計算成對比較矩陣的模糊權重

一旦決定各項風險的成對比較矩陣，將可進一步利用式(3)計算第一階層三大類別的模糊權重值及各相對之第二階層各項風險屬性的模糊權重值，其結果如表 2 所示。

(五)解模糊化

依據表 2 的結果，接著需進一步進行一致性檢定。首先，利用式(5)之 SLIDE 法對群體整合過後的第一階層三大類別及各個類別下第二階層所屬屬性之模糊成對比較矩陣內的各項模糊數進行解模糊的運算，接續前例， $\tilde{B}_1$ 解模糊的運算結果 B_1 為：

$$B_1 = \begin{bmatrix} 1 & 2.95 & 0.34 \\ 0.34 & 1 & 0.20 \\ 2.95 & 4.93 & 1 \end{bmatrix}$$

(六)一致性檢定

依據解模糊的結果，本研究利用 MATLAB ver.22 求得第一階層三大類別「法律」、「政策及組織帶來的風險」、「技術風險」及各個類別下第二階層的成對比較矩陣之特徵值（eigenvalue），經一致性檢定，由表 3 中，第一階層三大類別「法律」、「政策及組織帶來的風險」、「技術風險」的 C.I.與 C.R.值為 0.0160 與 0.0276，且 λ max（成對比較矩陣中最大特徵值），其值為 3.0320。「法律」類別下第二階層的 C.I.與 C.R.值為 0.0390 與 0.0434，λ max 為 4.1171。「政策及組織帶來的風險」類別下第二階層的 C.I.與 C.R.值為 0.0723 與 0.0548，λ max 為 7.4338。「技術風險」類別下第二階層的 C.I.與 C.R.值為 0.0583 與 0.0374，λ max 為 13.7002。結果顯示各個類別下第二階層的 C.I.與 C.R.值均小於 0.1，表示專家的評估偏好符合一致性的要求。利用式(5)之 SLIDE 法針對表 2 中的第一階層三大類別及各個類別下第二階層所屬屬性之模糊權重值進行解模糊，而得到解模糊後的類別與屬性權重值，其結果如表 3 所示。

(七)整體層級權重計算與排序

最後，利用式(6)，針對第一階層三大類別及各個類別下第二階層所屬屬性之權重值進行層級串聯得到整體層級權重，並依重要性程度的大小進行風險排序，其結果如表 3 所示。

經由解模糊化後求得三大類別之權重，依序為「法律」、「政策及組織帶來的風險」及「技術風險」。分析結果顯示，在於雲端運算服務風險威脅之類別中，第一排序為「法律」，為權重值最大。在「政策及組織帶來的風險」以及「技術風險」之前提，都要優先考慮到法律層面之問題，次要才是以公司企業及組織所訂定的政策與技術層面上的風險作為考量。雲端運算服務之二十四項風險屬性，整體排序之前五項之優先順序為「當地法院以傳票扣壓資訊硬體造成客戶資訊所有權問題」

表 3　雲端運算服務風險威脅屬性解模糊化相對權重值及整體排序

類別	類別權重值	屬性	屬性權重值	整體權重	整體排序
政策及組織帶來的風險	0.2913	服務遭封鎖	0.1832	0.05336	6
		喪失管理權	0.1122	0.03267	8
		改變承諾	0.3204	0.09332	3
		因租用客戶不法行動造成 ISP 名譽損失	0.0351	0.01021	16
		雲端服務遭終止	0.2314	0.06740	5
		ISP 更新裝備造成服務不穩定或終止	0.0340	0.00990	17
		供應鏈無法運作	0.0839	0.02443	9
		C.I.= 0.0723　C.R.= 0.0548　λmax = 7.4338			
技術風險	0.1063	資源耗盡	0.0976	0.01038	13
		客戶間資訊隔離失敗	0.1589	0.01689	10
		內部人員管理不當及濫權	0.1577	0.01676	11
		管理介面遭入侵	0.0522	0.00555	18
		客戶資訊遭攔截	0.0519	0.00552	19
		資訊在上傳或下載遭洩露	0.0231	0.00245	21
		資訊刪除不完整	0.0973	0.01034	14
		阻斷式服務	0.0228	0.00242	22
		阻斷式服務造成經濟損失	0.0152	0.00162	24
		遺失加密金鑰	0.0516	0.00549	20
		惡意的網路窺探或掃瞄	0.0170	0.00181	23
		雲端服務引擎遭入侵	0.0971	0.01031	15
		雲端服務環境無法滿足客戶安全要求	0.1575	0.01674	12
		C.I.= 0.0583　C.R.= 0.0374　λmax = 13.7002			
法律	0.6024	當地法院以傳票扣壓資訊硬體造成客戶資訊所有權問題	0.5050	0.30424	1
		管轄權變動的風險	0.2958	0.17820	2
		資料防護	0.1442	0.08690	4
		應用程式之軟體授權	0.0549	0.03310	7
		C.I.= 0.0390　C.R.= 0.0434　λmax = 4.1171			
C.I.= 0.0160　C.R.= 0.0276　λmax = 3.0320					

、「管轄權變動的風險」、「改變承諾」、「資料防護」、「雲端服務遭終止」。依據整體排序之前三項來進行探討與分析。

項目一、「當地法院以傳票扣壓資訊硬體造成所有權問題」：當客戶的資訊服務因違反當地法律，而遭到傳票扣壓資訊硬體，因客戶無擁有硬體財產權，但會造成雲端服務業者的硬體損失，建議資訊硬體在法定契約上應釐清所有權責，若硬體為租賃用途，更應注意契約條款，並盡量減少非法行為。

項目二、「管轄權變動的風險」：若雲端資料中心設置地點為一高風險國家（例如那些缺乏法治和法律框架的國家，缺乏遵守國際協定或規範等決心），導致資料強迫洩漏或系統受到扣押搜查，導致客戶資訊外洩，面臨法律問題。因企業無法直接管理雲端資料中心，但雲端資料中心的風險卻會帶來企業營運風險，建議在設置雲端資料中心時應盡量熟悉當地法律，慎重評估相關法律問題，並設計因應對策，次要才需評估資料中心之地點及機房設施以符合企業營運的計畫。

項目三、「改變承諾」：雲端服務業者與客戶的承諾是透過合約訂定，不可隨意改變。雲端服務業者或企業遇到問題，雙方均須按照合約條款執行。建議雲端服務業者應提供可實現的承諾，以及遵守相關標準或規範，並提供相關稽核（audit）資料備查。合約與稽核結果不僅可以協助雲端服務業者與企業雙方釐清雲端服務之風險威脅項目，還可由公正第三方將來做為導入雲端服務時風險評估之參考，以提升企業能在有限資源的範圍內，實現最佳化的資源分配並降低風險。

本研究結合模糊集合與層級分析法，假設每位專家對於風險屬性之意見可採用不相同的三角模糊，以代表其個人對屬性之風險偏好來進行探索性研究，使用模糊層級分析法求得各項屬性的相對權重值，解決在評估雲端服務之風險屬性之問題所具有的模糊性與不確定性，提升研究結果的準確性。經層級串聯後，將各項屬性之相對權重值依序做優先排序，說明權重值所反應出評估屬性的相對重要性，藉此可了解各屬性對於導入雲端服務評估風險時的重要性。藉由此分析，可以供企業管理者進行風險控管，減少企業在導入雲端服務時，因資安事件所帶來的威脅與衝擊。透過本研究的結果做為企業導入雲端服務時的參考依據。

伍、結論

本研究提出一套專案風險評估流程，合理評估與分析導入雲端服務專案之風險項目之優先順序及資訊資源的投資決策。本研究成果可協助雲端服務業者整體性的

資訊安全管理評估，了解雲端運算服務系統之風險所在，以利管理者動態評估系統風險，尋求適當管控措施（safeguards），降低系統風險；客戶可由雲端服務業者所提供的風險分析報告，作為在客戶導入雲端服務前的資安評估，認知導入後作業的風險性，以決定是否要採用雲端服務的部署方式未來研究方向將朝以下三個方向進行：(1)透過專案風險分析，以新型雲端運算的網路威脅如 APT，評估系統動態風險；(2)企業那些網路服務適合保留在企業內，那些網路服務適合移至雲端資料中心；(3)採用系統動態學（system dynamics）分析企業採用雲端運算之高風險的作業流程內威脅與衝擊損害的因果關係。

致謝

感謝兩位匿名審稿委員寶貴的意見使本文更具可讀性。同時，感謝行政院國家科學委員會支援本研究部份經費（計劃合約編號：NSC 99-2410-H-168-009）。

參考文獻

一、中文部份

1. 國際商業機器股份有限公司(2010)，IBM觀點：安全與雲端運算，國際商業機器股份有限公司網站，Retrieved February 17, 2012，取自：https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-TW_DP_SW&S_PKG=wp_securitycloudcomputing。

2. 王平、林文暉、郭溥村、王子夏、盧永翔(2010)，雲端運算服務之資安風險與挑戰，資訊安全通訊，16(4)，45-65。

3. 彭秀琴、張念慈(2010)，雲端運算下資訊安全之探討，經建會管制考核處，Retrieved February 17, 2012，取自：http://www.cepd.gov.tw/dn.aspx?uid=9857。

4. 黃富祿、張力允、李仁鐘、周碩聰(2010)，組織導入雲端運算之資安管理評估，資訊安全通訊，16(4)，66-83。

5. 鄭進興、陳堂昇(2010)，公路監理服務雲端運算與資安管理，資訊安全通訊，16(4)，94-111。

6. 劉家驊、洪士凱(2010)，雲端運算資料安全防護機制之研究，2010電腦視覺、影像處理與資訊技術研討會，桃園：清雲科技大學主辦。

7. 管孟忠(2011)，ISO 10006 專案品質管理系統的發展，開南大學專案管理研究所。

8. 蔡一郎(2010)，雲端運算與雲端安全架構，資訊安全通訊，16(4)，84-93。

二、英文部分

1. Chauhan, A., & Vaish, R. (2012). Magnetic material selection using multiple attribute decision making approach, Materials & Design, 36, 1-5.

2. Chapman, R. J. (2001). The controlling influences on effective risk identification and assessment for construction design management, International Journal of Project Management, 19(3), 147-157.

3. Chuu, S. J. (2009). Group decision-making model using fuzzy multiple attributes analysis for the evaluation of advanced manufacturing technology, Fuzzy Sets and Systems, 160(5), 586-602.

4. Cloud Security Alliance, (2010). Guidance for identity & access management V2.1, Cloud Security Alliance, 2010, Retrieved February 17, 2012, from https://cloudsecurityalliance.org/guidance/csaguide-dom-12.pdf.

5. Cloud Security Alliance, (2010a). Top Threats to Cloud Computing, Cloud Security Alliance, 2010, Retrieved February 17, 2012, from https://cloudsecurityalliance.org /topthreats/csathreats.v1.0.pdf.

6. European Network and Information Security Agency, (2010). Cloud computing: benefits, risks and recommendations for information security, European Network and Information Security Agency, 2010, Retrieved February 17, 2012, from http://www.enisa.europa.eu/act/rm/files/eliverables/cloud-computing-risk-assessment.

7. IBM (2009). Cloud Security Guidance IBM Recommendations for The Implementation of Cloud Security, Retrieved February 17, 2012, from http://www.redbooks.ibm.com /redapers/pdfs/redp4614.pdf.

8. International Organization for Standardization (2005). Information Technology-Security Techniques Information Security Management Systems-Requirement (ISO/IEC 27001).

9. Kuo, R. J., Wang, Y. C., & Tien, F. C. (2010). Integration of artificial neural network and MADA methods for green supplier selection, Journal of Cleaner Production, 18(12), 1161-1170.

10. Kutsch, E., & Hall, M. (2010). Deliberate Ignorance in Project Risk Management, International Journal of Project Management, 28(3), 245-255.

11. Laarhoven, P. J. M., & Pedrycz, W. (1983). A fuzzy extension of Saaty's priority theory, Fuzzy Sets and Systems, 11(1-3), 229-241.

12. Mabuchi, S. (1993). A proposal for a defuzzification strategy by the concept of sensitivity analysis, Fuzzy Sets and Systems, 55(1), 1-14.

13. Marques, G., Gourc, D., & Lauras, M. (2010). Multi-criteria performance analysis for decision making in project management, International Journal of Project Management, 29(8), 1057-1069.

14. Pang, J., & Liang, J. (2012). Evaluation of the results of multi-attribute group fecision-making with linguistic information, Omega, 40(3), 294-301.

15. Project Management Institute (2008). A Guide to The Project Management Body of Knowledge, Chapter 8 project risk management, 273-312, Fourth Edition, PA: Project Management Institute.

16. Saaty, T. L. (1978). Exploring the interface between hierarchies, multiple objectives and fuzzy sets, Fuzzy Sets and Systems, 1(1), 57-68.

17. Saaty, T. L. (1980). The Analytic Hierarchy Process, New York：McGraw-Hill.

18. Saaty, T. L. (1990). How to make a decision：The analytic hierarchy process, European Journal of Operational Research, 48(1), 9-26.

19. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, 34(1), 1-11.

20. Yager, R. R., & Filev, D. P. (1993). SLIDE：A simple adaptive defuzzification method, IEEE Transactions on Fuzzy Systems, 1(1), 69-78.

21. Zadeh, L. A. (1965). Fuzzy sets, Information and Control, 8(3), 338-353.

2012 年 **02** 月 **24** 日收稿

2012 年 **03** 月 **03** 日初審

2012 年 **07** 月 **27** 日複審

2012 年 **11** 月 **08** 日接受