行政院國家科學委員會專題研究計畫　期中進度報告

子計畫三:輕度障礙學生數學教學之數位學習平台核心模組與技術研發(1/3)

計畫類別： 整合型計畫
計畫編號： NSC94-2524-S-343-001-
執行期間： 94 年 05 月 01 日至 95 年 07 月 31 日
執行單位： 南華大學電子商務管理學系

計畫主持人： 王昌斌
共同主持人： 吳宗憲，何正得

報告類型： 精簡報告
報告附件： 出席國際會議研究心得報告及發表論文
處理方式： 本計畫可公開查詢

中　華　民　國 95 年 6 月 2 日

行政院國家科學委員會補助專題研究計畫期中報告

※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※
※　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　※
※　輕度障礙學生數學教學之數位學習平台核心模組與技術研發(1/3)　※
※　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：□個別型計畫　　■整合型計畫

計畫編號：NSC94-2524-S-343-001

執行期間：94 年 5 月 1 日至 95 年 7 月 31 日

計畫主持人：王昌斌　南華大學電子商務管理系

共同主持人：　陳裕民　國立成功大學製造工程研究所

吳宗憲　成功大學資工系

何正得　國立高雄應用科技大學工業工程管理系所

計畫參與人員：陳宗義 楊惠媚 鄭志新 南華大學資訊管理系所

南華大學資訊室

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份

□赴大陸地區出差或研習心得報告一份

■出席國際學術會議心得報告及發表之論文各一份

□國際合作研究計畫國外研究報告書一份

執行單位：南華大學電子商務管理系

中　華　民　國九十五年五月三十一日

一. 摘 要

數位學習的特色，在於受教者能打破時空限制，隨時隨地進行學習。經由數位學習，能使學習活動更有效率；加上教學內容可輕易大量複製，因能降低學習成本，達到「時時可學習（any time）」及「處處可學習（any where）」的學習目標。然而，目前尚無針對輕度障礙學生之教師、家長及相關領域專家之需求所發展之數學學科數位學習平台，能有效提供診斷與教學知識及教學策略與教材內容。是故，建構一知識管理導向之「輕度障礙學生數學教學之數位學習平台」實有必要性。

本計畫的主要目的是以輕度障礙學生數學教學之知識及知識管理之實現技術為基礎，來開發平台的核心功能模組與技術，並針對各模組之核心技術進行方法設計與元件開發，使平台具備：(1)提供教師適性化之教學策略、方法及教材之能力；(2)知識自動獲取、解析、儲存及自我學習之能力；(3)教學個案知識分析、學習樣板(Pattern)建立及預測之能力；(4)提供輕度障礙學生線上個人化自我學習之能力。

為達成上述研究之目的，本研究將進行下列主要研究項目：

(1) 設計功能模組細部架構，

(2) 發展一個具可適性化之教材內容標準及教材整合技術，

(3) 研發知識存取、知識擷取及可適性化教材之核心技術。

二. 計劃緣由與目的

2.1 研究背景

教育是國家百年大計；在這個知識爆炸的時代裡，教學成效的良窳，不僅影響諸多學子的一生，更攸關國家未來的發展前途。我們認為，教育的目的，不僅在培育揚名世界的精英學生，也應把焦點放在弱勢學生──學習障礙學生的身上。

學習障礙可分為閱讀疾患(reading disorder)、數學疾患(mathematics disorder)與文字表達疾患(disorder of written expression)等三類(陳以青，2004);而其中又以數學障礙最為普遍。國內外正式或非正式研究報告均指出，數學是國民中、小學學生最感學習困難的學科之一(邱上真、詹世宜、王惠川與吳建志，1995)。另研究報告也指出，國民中、小學學生約有6%具有嚴重的數學障礙(Fleischner , Marzola, 1988)。

數學為科學之母，是一切科學的基礎；欠缺數學能力的學生，未來勢與高新科技產業無緣。在可見的未來，勞力密集產業將從國內絕跡，欠缺數學能力者，極可能成為失業者的同義詞。因此，對數學學習障礙學生的誘導及訓練，使其能適應未來環境其具備獨立謀生之能力，不僅是當前特殊教育的努力目標之一，也是教育工作者的神聖使命與義務。

數學學習障礙難道真的無可挽救嗎？答案是否定的。研究指出：幾乎所有二年級數學學習障礙學生均有解題之潛能，惟教師必須發展適性化之教學策略，以增進學生成功的數學經驗（朱經明，2001）。但研究卻也顯示，大多教師面對數學學習障礙學生的問題時，常反覆使用先前未成功的教學策略，而未能針對個別的學習問題，使用不同教學方式(Fuchs et. al., 1991) 。

如前述，在資訊不發達的昔日，教師須以一己之力，在有限的時間內，對不同學生、不同主題發展適性化的教學策略以挽救學習障礙學生，顯然是力不從心。拜資訊科技之賜，今日，不同教師間經由網路交換教學心得，已不再是

夢想；倘能建構一數位學習(e-Learning)平台，讓所有面臨學習障礙學生的教師、家長，以及相關領域專家能在線上交換心得，進而能給予學習障礙學生適性的關懷與輔導，同時也提供教師即時的進修管道，以強化教師之學習障礙學生數學教學的專業知識與培養其適性化教學能力，不就有機會挽救這些學習障礙的學生了嗎？

是故，建構一知識管理導向之「輕度障礙學生數學教學之數位學習平台」，提供教師即時的進修管道，以強化教師之學習障礙學生數學教學的專業知識與培養其適性化教學能力，實有其價值與必要性。

數位學習的特色，在於受教者能打破時空限制，隨時隨地進行學習。經由數位學習，能使學習活動更有效率；加上教學內容可輕易大量複製，因能降低學習成本，達到「時時可學習（any time）」及「處處可學習（any where）」的學習目標。然而，目前的數位學習平台多以一般學生為教學對象，無法為前述學習障礙學生之教師、家長及相關領域專家，針對其面臨的個案，有效提供相關之診斷與教學知識及教學策略與教材內容。目前雖有相關研究，將學習者在教學平台上的學習行為，透過網站的紀錄檔(Log Files)資料加以探勘(Mining)，期能辨識學習者之學習行為樣式(Pattern)，以利後續教學策略的調整(張智凱,2002， 蔡昌均,2001)；然其研究對象是數位學習平台的直接使用者；本研究的對象──輕度障礙學生卻非平台的使用者。如何經由他人敘述，獲得、分析、存取與管理大量且異質性之學生身心特質知識、教學知識、教材與教學案例；仍待進一步深入探討。此外，使用介面若能由鍵盤或語音輸入，當可造福更多電腦操作障礙的相關使用者。以上種種，仍是亟待解決的問題，也是「輕度障礙學生數學教學之數位學習平台」成敗的關鍵。

為此，本研究將研發「輕度障礙學生數學教學之數位學習平台相關實現技術」，包括核心模組與核心技術研發。我們認為，數位學習平台的問世，是上天賜予學習障礙學生的最好契機；也是值得吾人全力以赴的研究領域。

2.2 研究目的

本研究之總目標在建構一知識管理導向之輕度障礙學生數學教學之數位學習平台，本(子)計畫的主要目的在開發平台功能模組與其核心技術，並針對各模組之核心技術進行方法設計與元件開發，使核心技術能具共用性、彈性及可再用性，使本平台具備：(1)提供教師「輕度障礙學生數學教學」之適性化教學策略、方法與知識及教材之功能；(2)知識自動獲取、解析、儲存及自我學習甚至之功能；(3)教學個案知識分析、學習樣板(Pattern)建立及預測之功能；(4)提供輕度障礙學生線上個人化自我數學學習功能。

為達成上述研究之目的，本研究將進行下列主要研究項目：

(4)設計功能模組細部架構:包含問題詢答 (User inquiry) 、知識分享 (Knowledge Sharing) 、個案診斷教學、知識擷取、專家庫與社群、學生線上個人化學習、學習評量、系統管理與維護。

(5) 發展一個具可適性化之教材內容標準及教材整合技術

(6) 研發下列核心技術：

- 知識存取控制(Access control) 技術
- 網路互動式問題與需求語意分析技術
- 知識擷取(Knowledge Mining) 技術
  - (a)案例知識探勘與行為分析技術
  - (b)個案學生學習歷程分析與個案知識探勘
  - (c)專家知識擷取(Expert Knowledge Capturing)
  - (d)網路知識探勘(Web Knowledge Mining)
- 學生線上個人化學習機制 (與子計劃一持續密切進行中)
- 適性化教材之建構及產生技術 (與子計劃一持續密切進行中)

本(子)計畫共依序執行三年，第一年之預期產出如下：

（1）平台之主要功能與功能模組之細部架構

（2）語意分析與知識轉換技術

（3）知識存取權限與技術之研究

（4）一個具可適性化之教材內容標準及教材整合技術(與子計劃一合作)

（5）個案學習歷程庫模型及各類知識庫模型 (與子計劃二合作)

三. 目前研究成果

本(子)計畫第一年之完成項目包括:

（1）輕度障礙學生數學教學之數位學習平台架構與功能模組之設計及系統開發

（2）網路互動式問題與需求語意分析技術

・自動摘要數位學習平台討論區內容機制設計

・網路資料與知識萃取技術之研究

（3）知識存取權限與技術之研究

3.1 輕度障礙學生數學教學之數位學習平台架構與功能模組之開發

本數位學習平台乃針對輕度障礙學生之數學教學目標與欠缺之處，分析教育專家、教育工作者、家長及學生之需求及各成員與平台之間的互動，設計一個能提供教育工作者適性化教學策略、方法及教材之平台，提供輕度數學障礙學生線上診斷與學習之環境，藉以提升教學效益並解決現階段學習過程中輕度障礙學生所遭遇之學習障礙。茲分別說明「數位學習平台整體架構之需求」、「數位學習平台整體架構之設計」、「數位學習平台整體架構之主要功能模組」、「數位學習平台整體架構之使用者介面設計」如下：

(1)數位學習平台整體架構之需求

數位學習為一知識推播與擴散的程序，其與傳統教學方式的主要差異，在於結合資訊科技與網際網路以彌補傳統教學模式的不足與缺陷；當前許多數位學習實務過分強調資訊技術的導入與應用，恐將造成偏重功能面的「技術導向型數位學習平台」，而失去教學的本質與目的。因此，若能以「學習理論與教學理論」為核心，以「知識管理」為基礎，進行數位平台的規劃與設計，將數位學習視為知識導向與知識密集的活動，並以知識管理之理念為核心，落實知識

獲得、分析、存取、管理、分享、演繹與創新，方能實現數位學習之目標，並顯現其價值。

因此本計畫將結合「知識擷取」、「知識儲存與管理」、「知識分享與擴散」及「知識整合」等知識模組與元件，整合異質知識來源與內容，提供適性化與動態化的教學服務，本計畫提出一個「知識管理導向數位學習模式」，詳細內容請參閱附件(一)。

(2)數位學習平台整體架構之設計

本數位學習平台設計考量之依據：輕度障礙學生之特性、教育輕度障礙學生之教學支援需求、及目前之網路、語音與多媒體線上教學技術之應用，配合子計畫(一)「輕度障礙學生數學教學之數位知識內容建構」及子計畫(二)「輕度障礙學生數學教學之數位學習平台知識管理實現技術研發」之研究成果，結合核心模組與技術研發等相關工作而架構之輕度障礙學生數學教學之數位學習平台。

本平台之主要功能模組包括:功能介面、核心模組、知識管理引擎、數位知識內容儲存區四層；功能介面包括: 個案診斷教學、知識分享、問題詢答、受輔學生線上學習、專家庫與社群及系統管理；知識管理實現元件包括: 知識儲存、知識撿索、個案診斷教學推理、系統自我學習與內容維護；數位內容儲存區將儲存之數位內容包括: 數位知識、教學案例及個案診斷與學習歷程資料。本計畫以系統配置、系統架構、系統功能模組與細部系統功能架構等詳細規劃了數位學習平台整體架構，詳細內容請參閱附件(二)、請觀摩輕度障礙學生數學教學之數位學習平台(網址：http://203.72.1.53:8080)。

3.2 網路互動式問題與需求語意分析技術

目前本計畫在網路互動式問題與需求語意分析技術上可分為兩個研究領域：「自動摘要數位學習平台討論區內容機制設計」與「網路資料與知識萃取

技術之研究」，分別敘述如下：

(1)自動摘要數位學習平台討論區內容機制設計

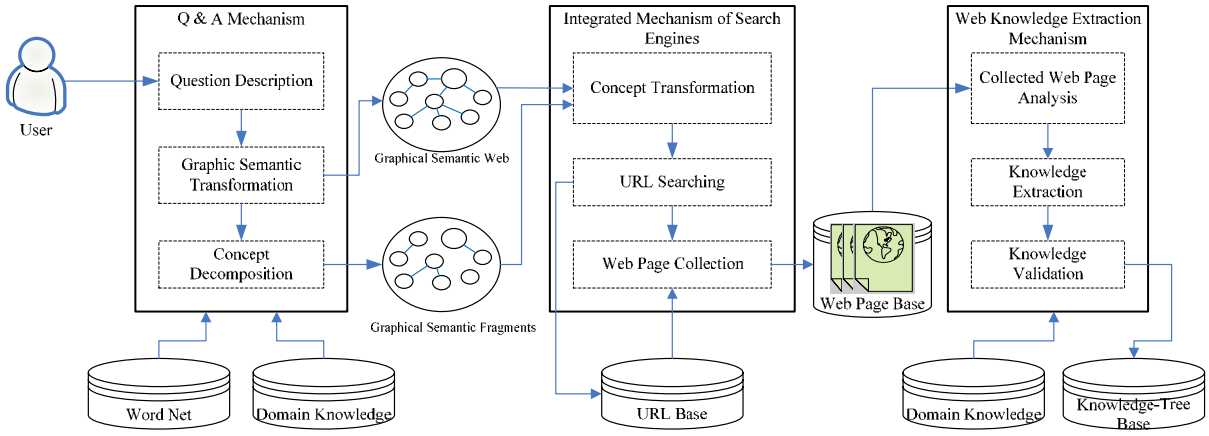
由於數位學習模式不像傳統的教學模式,可以容易讓老師與學生實際面對面的接觸，所以老師與學生的交流有一定的限制。LERN(1998)曾提出數位學習平台主要有7種服務，其中提到，若要方便課程討論與師生互動的服務，必須組織網路論壇(Forum)區；另外也提到，可運用電子佈告欄(BBS)、討論區等服務針對特定議題分享不同觀點。因此討論區成為數位學習平台上有效讓老師與學生、學生與學生間的重要互動服務。當學生發生問題時，學生可以在平台上詢問，或是互相討論課業，老師也可以透過學習平台發佈學習進度，或是為學生解答疑惑。

目前討論區充滿大量互動的資訊供師生學習與分享，但由於資訊過量，使得師生需花費大量的時間尋找所需的資訊。而研究中指出，這些資訊隱藏著許多有用的知識，目前是透過人工的方式將資訊整理成知識，費時費力。爲了降低人工方式整理的人力與搜尋的時間，本研究利用CKIP的中文斷詞服務及GBP方法設計一個自動摘要數位學習平台討論區內容機制，將討論區內容彙整並摘錄重點產生成FAQ，以輔助網站管理者或討論區版主輕鬆地及有效率地進行知識擷取與轉換的工作環境，並快速有效率的將討論區中的知識分享給所有的師生使用，詳細內容請參閱附件(三)。

(2) 網路資料與知識萃取技術之研究

傳統教學受限於時間與空間，隨著科技及網際網路時代的來臨，數位學習平台可解決傳統教學所面臨的困難，而網路上充滿著豐富的知識，如何以自動化的方式有效的利用網路上的資料提供使用者所需的知識是一項很大的挑戰。針對此一問題，設計一個智慧型之網路知識擷取及建構機制的系統架構，如圖一所示，此架構主要包含三個部分：(1) 使用者語意分析機制(Semantic Analysis

Mechanism，SAM)、(2) 整合式網頁搜尋引擎機制(Integrated Mechanism of Search Engines on Web)和(3)網頁知識擷取及建構機制(Knowledge Extraction and Construction Mechanism)。



圖一 網路資料與知識萃取之架構

所設計之架構能夠解析出使用者所提出之問題的涵義並找出以不同語法及同義字的表達方式，將原始的問題轉成一個圖形化的語意網路模型，以此模型來描述使用者所提出問題的概念；以此模型再配合整合式搜尋引擎機制來進行相關知識的搜尋，找出符合使用者問題之網頁；透過知識擷取機制擷取相關的知識，進一步建構成知識樹，最後將知識回覆給使用者。從學習者(使用者)的觀點分析網路資料與知識萃取架構的運作，步驟如下：

Step1：學習者以自然語言方式輸入待解的問題。

Step2：問題透過中文斷詞處理後，形成關鍵詞與圖形化語意概念圖。

Step3：在數個搜尋引擎中以關鍵詞搜尋相關網頁。

Step4：搜尋的網頁以標準化方式加以儲存。

Step5：將網頁內容與圖形化語意概念圖加以比對與篩選。

Step6：擷取網頁內容並建構成知識樹加以儲存。

Step7：將知識交由專家評定與驗證。

Step8：將知識傳達給學習者

網路資料與知識萃取技術架構與相關技術之研究將針對該架構所組成之「問題與需求語意分析」、「網路知識搜尋與過濾」與「網路知識編譯與擷取」分別說明之：

- **使用者問題之語意分析機制**

人們遇到問題時，往往會藉由搜尋引擎來尋找相關資訊，因此，透過網際網路獲取資源已成為數位學習有利的工具之一，藉由搜尋引擎之便找尋相關資訊，不僅迅速與方便，同時可以解決資訊匱乏的問題。然而，當使用者有問題時想獲得精確的答案時卻總是不得其門而入，可能輸入關鍵字後獲得許多雜亂的資訊，或是當使用者對此領域不了解時輸入關鍵字卻找不到想獲得的資訊，無論是在怎樣的平台上搜尋許多使用者都遇到這樣的一個問題，目前只能依靠使用者對於搜尋的資料逐步的輸入相關的關鍵字來搜尋所需問題之解答。

本研究提出一方法來解析出使用者所描述問題之語意，利用斷詞規則發現自然語言之關鍵字，以統一模型語言(Unified Modeling Language，UML)中之類別圖關係來建構出語意網概念模型，配合 ontology 技術加以延伸出更廣闊之概念，將建構的概念加入權重及過濾，最後以圖形化語意網表示，不僅可以讓使用者了解問題所衍生的語意，更可以讓使用者與電腦進行有效的溝通，進而轉成電腦可理解的語意,搜尋出使用者真正所需的資料,詳細內容請參閱附件(四)。

- **網路知識搜尋與過濾**

網路上的資訊是屬於一個超大型資料庫，能提供查詢服務的資訊軟體系統，稱為搜尋引擎(search engine)，透過網際網路獲取資源已成為數位學習有利的工具之一，藉由搜尋引擎之便找尋相關資訊，不僅迅速與方便，同時可以解

決資訊匱乏的問題，但是由於目前搜尋引擎所搜尋之知識量往往重複性太高，甚至有搜尋結果不符合需求的情況發生，既浪費頻寬且效能大幅降低。由於知識的蒐集、獲取、整合、儲存、管理、分享與運用之重要性與日驟增，如何正確的從使用者的觀點透過網路獲取正確的資訊且有效率地轉化成知識是學者長久來所追求目標之一。

利用前述之技術擷取出使用者自然語意問題之關鍵字，利用搜尋引擎(search engine)尋找相關資訊，並結合網頁內容探勘(web content mining)、資訊檢索(information retrieval)相關技術與導入領域實體(domain ontology)概念，針對搜尋後的摘要及標題進行資訊含量之計算，透過相關演算法過濾格式不完整、重覆性與廣告之內容，其後依資訊含量給予權重與排序，提供給使用者較貼切原意的網頁內容，進而提供相關性與重要性的參考，希望可有效避免使用者浪費精神與時間自行過濾檢索，詳細內容請參閱附件(五)。

- **網路知識擷取**

當學習平台之知識庫或教材庫無法滿足學習者知識的需求或解決問題時，則須由專家增加教材庫或知識庫的教學內容(content)，無法滿足立即回饋的需求。因此，本研究將設計網路知識擷取及建構之機制，此機制不僅能有效改善教學平台有限的知識庫或教材庫之不足，而且能使知識庫隨著使用者的使用不受限制的向外延伸及深入問題的核心。但如何以自動化的方式針對學習者想了解的問題，在網路上搜尋答案進而建構成一個有組織有系統的知識庫用於支援學習者進行學習的活動是一項大的挑戰。

利用前述問題與需求語意分析、網路知識搜尋與過濾之技術，提供給使用者較貼切原意的網頁內容，可以避免使用者浪費精神與時間自行過濾檢索，但是對於網路知識之儲存與最短時間內將不同的知識來源組合呈現給使用者仍有改進之空間，因此本機制乃藉由本體論與自然語言處理的結合把使用者所輸入的詢問句子分析，再將網頁內容與學習者的問題進行比對，不僅可依照其網頁內

容分群讓使用者能更迅速的找到所需的文件，而且可以經過一連串的擷取程序找出各文章中符合的段落進而組成知識，甚至可以進行知識呈現與驗證的工作。透過上述之程序，期望能以最適性化的方式將隱含在網路中的知識提供給使用者，達到網路知識擷取與知識分享之目的，詳細內容請參閱附件(六)。

3.4 知識存取權限與技術之研究

知識存取控制(Access control) 技術研發：在開放式的網路環境下，此知識存取控制技術能提供適當的知識分享及維護學習障礙學生個案資料的安全，是一個兼具知識安全及分享的存取控制機制。為開發本核心元件，主要研究項目必須分析本平台之資訊及知識的使用與分享模式及「Web-based資訊環境」資源管理的需求，進而提出適合本平台需求之「存取控制模式」，設計「知識分類技術」，可考慮以「類神經網路」或「模糊理論」來進行「知識分類元件設計」。根據模式分析的結果，探討目前已被提出之存取控制模型（包含隨意型存取管制、嚴格型之存取管制、角色為基之存取控制模型或任務為基之存取控制模式等），選擇一個適合本平台之「權限管理存取控制模型」，並進行改善工作，進而提出一個「知識存取控制模型」。之後，以物件導向之分析與設計方法進行此核心元件的開發工作。

此部分之研究目前已有兩篇文章發表於SCI (accepted 2006)，此兩篇文章主要以行動企業存取控制為重點，將來可被應用於本系統之安全控制，詳細內容請參閱附件(七)、附件(八)。

四、結論與討論

本(子)計畫第一年之完成項目包括:

（1）輕度障礙學生數學教學之數位學習平台架構與功能模組之設計及系統開發

（2）網路互動式問題與需求語意分析技術

・自動摘要數位學習平台討論區內容機制設計

・網路資料與知識萃取技術之研究

（3）知識存取權限與技術之研究

第二年將以系統功能模組開發為重心，第三年則將完成(1)各子計畫模組與機制整合及(2)系統整合、測試與平台導入。

五、相關著作

本計畫完成之期刊論文與研討會論文如下：

期刊論文

1. Tsung-Yi Chen, Yun-Min Chen, Chin-Bin Wang and Hui-Chuan Chu, Development of an Access Control Model, System Architecture and Approaches for Information Sharing in Virtual Enterprise, Computers in Industry. (Accepted) 2006 (SCI/EI)
2. Tsung-Yi Chen, Yun-Min Chen, Hui-Chuan Chu and Chin-Bin Wang and Huimei Yang, Resource Sharing to Support Cross-Organization Collaboration in Virtual Enterprise Using a Novel Trust Method, Robotics and Computer-Integrated Manufacturing. (Accepted) 2006 (SCI/EI)

研討會論文

1. Chin-Bin Wang, Huimei Yang, Yuh-Min Chen, Hui-Chuan Chu, Tsung-Yi Chen, Derchian Tsaih, An Intelligent Web Knowledge Extraction Framework to Support E-Learning Content Collection World Conference on E-Learning in Corporate, Government, Healthcare, & Higher Education 2006 Honolulu, Hawaii

2.應用領域知識設計網路上整合式搜尋引擎機制於數位學習方面,2006年第二屆全國數位內容學習研討會,立德管理學院

附件(一) 知識管理導向數位學習模式

1. Introduction

1.1 研究背景

隨著資訊科技的蓬勃發展，及網際網路環境的日益普遍與深化，整合網路與資訊技術的新型態數位學習模式，已形成一股新興的趨勢，也為全球各主要國家推動教育升級與改革的重要策略與方針，如美國政府推動之 ADL(Advanced Distributed Learning)(SCORM, 2003)、國際電機電子工程師協會提出之 IEEE LOM(IEEE Object Metadata)(LTSC, 2004)、與德國所發展的 LMML(Learning Material Markup Language)(LMML, 1999)等。由先進諸國競相投入大量資源於此領域可知，數位學習將在本世紀之教育領域中扮演重要角色。

數位學習可定義為『利用電腦科技進行的遠距學習』(Henderson, 2003)。有別於傳統師生間面對面的學習模式，透過數位學習工具，學習者可突破時間與空間的限制，進行遠距離與非同步的學習活動(Hwang, 1998；Sun & Chou, 1996)；而傳統紙本的教學內容在經過數位化的轉換程序後，將更易於編修、彙整、互通及整合(Rosenberg Marc, 2001；Urdan & Weggen, 2000)，大幅提升其再用性(Reusability)與分享性(Share)；此外，藉網路串連所形成的網路學習社群(e-Community)，也可透過社群成員間密切的互動、諮詢、分享與討論，成為一即時性的知識來源與管道。

1.2 研究動機

近年來，經由產官學界的積極推動，數位學習環境已漸趨成熟(蔡昌均、曾憲雄等，民 91；朱治平，張慶寶等，民 92)，數位學習平台相關功能的設計與開發也日益完備，學習者已可初步領略數位學習所帶來的便利與樂趣。然而許多

數位學習平台，存有下列三項缺陷(Antal, 1997；Principe et al., 1998)：(1)缺乏適性化的教學模式與動態的教學內容；(2)缺乏跨領域教學知識及內容的整合能力；(3)缺乏教學案例與知識的自我修正與回饋之機制；成為發展數位學習的障礙。另有學者指出，學習系統的設計者會面對的困難之一，就是如何能儲存教學過程中必備的大量知識；而知識管理的相關理論，恰能提供設計之是儲存區的指引與參考(Huerta, 2003）。

數位學習為一知識推播與擴散的程序，其與傳統教學方式的主要差異，在於結合資訊科技與網際網路以彌補傳統教學模式的不足與缺陷；當前許多數位學習實務過分強調資訊技術的導入與應用，恐將造成偏重功能面的『技術導向型數位學習平台』，而失去教學的本質與目的。因此，若能以『學習理論與教學理論』為核心，以『知識管理』為基礎，進行數位平台的規劃與設計，將數位學習視為知識導向與知識密集的活動，並以知識管理之理念為核心，落實知識獲得、分析、存取、管理、分享、演繹與創新，方能實現數位學習之目標，並顯現其價值。

『知識管理』係指組織或個人在面對非連續變化時，將原本存在於組織內知識工作者或隱藏於制度、資料庫、文件、歷史資料之中的知識加以分辨、獲取、選擇、儲存、管理、應用、創造與分享 (Demarest, 1997)。在實務上，『知識管理』為資料收集、組織內知識的分享、管理資訊系統(MIS)、流程管理以及學習經驗等的整合，為一系統化的知識累積過程，同時有效的運用知識，並不斷地持續強化所累積的知識，使個人以至於整個組織均能因知識的普及而進步，達成更高的效能。在可見的未來，知識進步必將一日千里，數位學習平台更須具備知識獲得、分析、存取、管理、分享、演繹與創新之機制，方得提昇數位學習之效益，因此知識管理導向之數位學習為未來必然之趨勢。

1.3 研究目的

綜上，一個理想之數位學習平台，須具備『知識擷取』、『知識儲存與管理』、『知識分享與擴散』及『知識整合』等知識模組與元件，以整合異質知識來源與內容，提供適性化與動態化的教學服務；此外，現行數位學習平台亦仍存有若干盲點或問題亦待解決。有鑒於此，進行研究如下：

1. 提出一「知識管理導向之數位學習模式」

2. 設計一「知識管理導向之數位學習平台系統架構」

期能提供知識表達、儲存、推理、維護與學習機制，以更有效地將知識轉化為學習內容，進一步提升數位學習效能。

2. Learning, e-Learning, and Knowledge Management

2.1 Learning and Theories

2.1.1 Learning

一般心理學家對學習(Learning)之定義，係指「藉由經驗，使行為發生持久性的改變」(Weiss, 1990)。前述定義中，學習涉及「行為的改變」；若僅是思考過程或態度改變，但是行為依舊，那並不能稱為學習。此外，學習必須經由某些經驗的認知，可能是透過直接的觀察或實習，也可能是透過間接的方式，如閱讀書籍。如果此經驗能造成行為改變，就可確定學習已發生了。(Robbins, 2001)

2.1.2 Learning Theories

不同學派的心理學家曾對學習提出不同的理論解釋，但是這些理論通常被歸納為(1)行為式(behavioral)與(2)認知式(cognitive)兩種(Leidner et al., 1995)：行為學派心理學家把學習時的行為改變，解釋為刺激與反應間的連結，要經由後

效強化的方式來達到學習效果，此稱之為連結論(association theory)，代表人物為提出操作制約(operant conditioning)理論的斯金納(B. F. Skinner)；認知學派心理學家則把學習時的行為改變，解釋為認知結構的獲得與重組，將個體對環境事物的認識與了解，視為學習的必要條件，其理論則稱為認知論(cognitive theory)，代表人物有提出「認知學習論」的皮亞傑(J. Piaget)與提倡「發現學習法」的布魯納(J. S. Bruner)等。以下就分別討論斯金納與布魯納的理論。

2.1.2.1 斯金納的理論

斯金納的教學理論以操作制約為核心觀念，認為教學(teaching)是藉由安排增強的構成情境，使學習者得到一些對他將來有用的行為。

斯金納將操作制約原理應用到教學上，衍生出：(1) 正增強 (2) 消弱 (3) 塑造 (4) 間歇增強 (5) 刺激控制 (6) 類化 (7) 串連 (8) 消褪 (9) 懲罰 (10) 逃脫與躲避 等十個原理為教學要點，並以直線編序、機器輔助的「編序教學法」(Programmed Instruction)為其實用方法。

斯金納指出，若有適當的教學機配合良好的編序內容，編序教學將可具有下列優點：

1. 可以讓學生一直主動進行學習，並排除外因的干擾；
2. 可以立即增強正確的反應，使學生獲得成就感；
3. 可以免去嫌惡的控制；
4. 老師可以巡視全班，學生可以依照自己的速度學習；
5. 請假或生病的學生，可以隨時繼續學習，不必擔心趕不上進度；
6. 漸進的安排，學生可以逐步學會複雜的行為；
7. 可以讓學生完全貫通教材內容

然而編序教學法另有以下缺點：

1. 受器材與設備限制，不可能完全普遍採用；(張春興、林清山, 1996) 且師生不見得都具有排除設備故障的能力，可能因設備故障而延誤學習。
2. 教材編製不易：編序教材編製極為困難，也不是所有科目都能編成漸進式的零碎題目；若勉強使用，難免使知識失去系統性，學不到事理的整體觀念；(張春興、林清山, 1996)
3. 缺乏教師的影響力：教師在教學活動中，除了傳授知識技能外，也影響學生的態度、觀念、價值判斷等；若只靠機器傳遞知識，便喪失了教育中的重要意義；(張春興、林清山, 1996)
4. 缺乏教育歷程中的社會功能：教學過程中，除師生授受關係之外，同學之間的競爭，合作、感情、友愛等社會關係，對學生的知能、社會、人格等各方面發展，均有影響作用。編序教學法(張春興、林清山, 1996)
5. 編序教學法採取有效的學習方式，反對嘗試錯誤，這固然可以提高學習效率，卻也忽略了學習過程；因而會限制學生思考範圍，有「知其然，不知其所以然」的問題，也不適合用來教授尚在發展中的學科。
6. 由於教材編製不易，也就導致教材內容更新的困難。

2.1.2.2 布魯納的理論

布魯納以認知理論為基礎，認為學習是一種由學習者主動參與處理訊息並將訊息加以組織和建構，使納入學習者心目中代表「真實世界之模型」(model of reality)之歷程。布魯納提倡「發現學習法」 (Discovery Learning)，鼓勵學生進行直覺思考、比較、對照，以激發學生對問題之好奇心，再誘導學生自行探索答案，並在探索過程中學得學習的技能。

發現學習法有下列優點：(張春興、林清山, 1996)

1. 引導學生主動自發的學習：教學過程中，引導學生主動學習，學生不僅學到知識，還學到對問題困境的主動適應態度、思考方法，以及解決困難的能力。
2. 有助於學習遷移：由發現過程中習得的知識，不但保持長久，也容易在日後類似的情境中產生學習遷移；可以觸類旁通，擴大學習效果。
3. 容易維持學習動機：學生的學習動機係來自發現的結果，因此不必假借外在的獎懲手段去強制達到教學的目的。

然而發現學習法也有下列缺點：

1. 適用學科受限：發現學習法對於「不必知其所以然」的知識無效。
2. 適用對象受限：對於缺乏主動學習意願的學生，不適合採用發現學習法。
3. 進度不易掌握：由於學習過程以學生為主體，教師只是站在輔助角色；並無法預知學生的發現過程需要多少時間，對於有時間限制的教學並不適用。

2.1.3 Experiential Learning Cycle

Kolb (1984) 綜合了Dewey的哲學實用主義(philosophical pragmatism)、Lewin的社會心理學與Piaget的認知發展理論，提出其經驗學習理論(Experiential Learning Theory, ELT)，該理論定義學習為一種透過經驗轉化而創造知識的過程，是一種持續的歷程而不是結果。其所以強調經驗(experiential)，是用以區隔過度強調認知影響的認知學習理論，以及否認所有內在體驗的行為學習理論。

Kolb將經驗學習分為具體經驗(Concrete Experience)、省思觀察(Reflective Observation)、產生新觀念(Abstract Conceptualization)與實際運用新觀念於新經驗(Active Experimentation)四個階段的循環，稱之為經驗學習循環(Experiential Learning Cycle)，如下圖2.1。

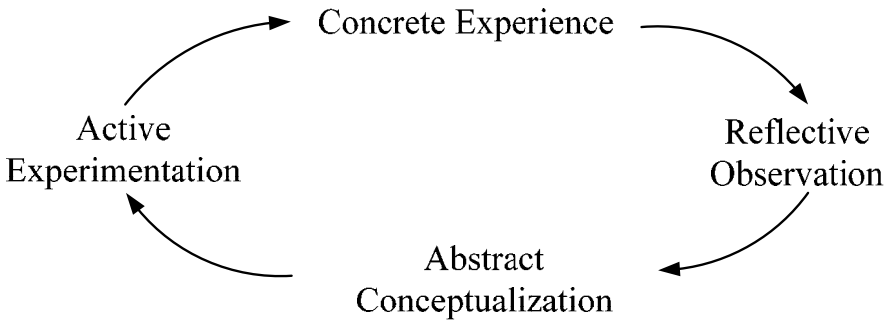


Figure 2.1　Experiential Learning Cycle (Kolb, 1984)

2.2 e-Learning

2.2.1 e-Learning：定義與發展

有別於傳統面對面的學習模式，數位學習係透過數位學習工具與網際網路，使學習者可突破空間與時間的限制，進行遠距離與非同步的學習活動(Hwang, 1998; Sun & Chou, 1996)；此外，傳統紙本的教學內容在經過數位化的轉換程序後，將更易於編修、彙整、互通及整合(Rosenberg Marc, 2001; Urdan & Weggen, 2000)，大幅提升其再用性(Reusability)與可分享性(Shareability)。

數位學習可定義為『利用電腦科技(通常在網際網路上)進行的遠距學習』(Henderson, 2003)。Moore 等學者則將數位學習定義為：數位學習是有計劃的學習，通常學習者與教學者分隔兩地；因而必須採用特殊的課程設計及教學技巧、特殊的電子或其他科技傳播方式，以及特殊的組織與行政作業配合，方能達成。(Moore et al., 1996)。Rosenberg 則認為數位學習是網路化的學習，藉由網路零距離、零時差的學習便利性，員工可以即時更新、存取、散佈、及分享教學的內容或資訊(Rosenberg, 2001)。由於訓練時間與地點的限制逐漸消失，透過線上學習，員工可以在任何時間進行學習活動，自由安排上課時間，在不影響員工上班情緒、不加深員工負擔的原則下，提高員工生產力。

近年來，數位學習日益受到重視，除了企業職訓之外，學校教育也逐漸導入數位學習的方式來進行教學。透過數位學習，使得學習活動更加有效率，以降低學習成本，落實『隨時學習(Any Time)，隨處學習(Any Where)』的學習模式，俾達終身學習的理想。

2.2.2 e-Learning：特性(features)與問題

為協助使用者達成學習目的，今日的數位學習已發展出許多特性(features)，如互動性(interactivity)、真實性(authenticity)、自主控制(learner-control)、便利(convenience)、自我導向(self-containment)、便於使用(ease of use)、線上支援(online support)、課程內容安全性(course security)、富成本效益(cost effectiveness)、協同學習(collaborative learning)、提供正式與非正式學習環境(formal and informal environments)、跨領域(multiple expertise)、線上評鑑(online evaluation)、線上搜尋(online search)、隨處可用(global accessibility)、跨文化互動(cross-cultural interaction)、有教無類(non-discriminatory)等特性(Khan, 2005) 。並且隨著資訊科技進步，這些特性仍不斷增加中。

儘管有上述特性，數位學習仍存有不少問題。學者 Bonk 等人(2004)彙整文獻，列舉進行數位學習時常見的十點問題：(Bonk et al., 2004)

1. 對於缺乏經驗的學生，數位學習往往會嚇倒新進學習者。
2. 即使是具有相當技術背景的學生，也可能會感到困惑或迷失在網路之中。
3. 網路上的學生彼此間都很客氣，這可能是由於缺乏面對面的互動與共同的體驗所致——然而，這樣會缺乏同儕的刺激而影響學習成效。
4. 學生們在線上常講些毫無根據的事；此外，學生有時會發表一些與課程無關的言論。

5. 在網路上教學很難不說教，也因此常常偏離了數位學習應以學習者為中心的原則。
6. 網路上的同儕不如教師貼心。
7. 難以在學習者間建立社群——可能是因為學生極端的任務導向(task oriented)，而非討論導向(discussion oriented)；也可能導因於大多的數位學習環境中，缺乏建立社會關係與互信的活動，也因此缺乏同儕關係。
8. 有太多的資料/資訊要讀，根本無法對學生一一回應。
9. 教師對學生的線上討論內容評分相當耗時。
10. 技術變化太快，或始終無法趕上需求。也常發生如伺服器無法存取、電腦當機、程式無法運作等狀況。此外，軟體的 Bug 與小錯誤都會讓學生感到挫折。

2.2.3 e-Learning 與 Knowledge Management

數位學習是一種知識活動，是故數位學習與知識管理有關，然而兩者並不相同。知識管理是為有經驗、較熟練的使用者而設計；而數位學習則是為新手而設計的，因此需要較為仔細的學習引導。兩者雖有部份重疊，但並非為同一類使用者而設計的 (Henderson, 2003)。數位學習與知識管理兩者的重疊關係已廣為人知，若干企業正試圖進行兩者之整合，以充分發揮學習資源並消弭多餘的活動。(Morrison, 2003)

許多數位學習平台，存有下列三項缺陷(Antal, 1997；Principe et al., 1998)：(1)缺乏適性化的教學模式與動態的教學內容；(2)缺乏跨領域教學知識及內容的整合能力；(3)缺乏教學案例與知識的自我修正與回饋之機制；成為發展數位學習的障礙。前節所列的十點問題，其實有數點(第 1, 2, 5, 8 點)即此三項缺陷所致。當前許多學習系統的設計者會面對的困難之一，就是如何能儲存教學過程中必備的大量知識；而知識管理的相關理論，恰能提供設計知識儲存區的指引

與參考(Huerta, 2003）。

數位學習為一知識推播與擴散的程序，其與傳統教學方式的主要差異，在於結合資訊科技與網際網路以彌補傳統教學模式的不足與缺陷；但若過分強調資訊技術的導入與應用，將造成偏重功能面的『技術導向型數位學習平台』，而失去教學的本質與目的。因此，若能以『學習理論與教學理論』為核心，以『知識管理』為基礎，進行數位平台的規劃與設計，將數位學習視為知識導向與知識密集的活動，並以知識管理之理念為核心，落實知識獲得、分析、存取、管理、分享、演繹與創新，方能實現數位學習之目標，並顯現其價值。

2.3 Knowledge Management

2.3.1 知識

知識是難以形容的，因為知識存在於不同的形式中；有些是無法消化的，因為我們根本無法想像知識是什麼，也不知道知識是如何形成的。(Demarest, 1997)

知識擁有多重涵義，也常與資訊相互混淆。Machlup(1983)對資訊下了註解，指出資訊是一連串的訊息與意義，可以增加、架構或是改變知識；而知識則是經由整合一連串資訊而產生的(Nonaka, 1994)。Bergeron 也指出，知識是為了提高理解(comprehension)、認知(awareness)、了解(understanding)而被組織(organized)、合成(synthesized)、歸納(summarized)的資訊。(Bergeron, 2003)

知識的特殊性使其與其他資源完全不同。學者 Wiig 等人將知識的特徵歸納如下：(Wiig et al., 1997)

1. 知識沒有實體且難以測量。

2. 知識容易揮發，它可能憑空消失。

3. 知識大多可在意志(Wills)下具體化。

4. 知識不會在使用過程中消耗，反可能因使用而增加。

5. 知識在組織中有大範圍的影響力。(知識就是力量)

6. 知識不能隨時上市，它通常有相當長的前置期。

7. 知識具非敵對性(Non-rival)，因為它可以在同一時間用在不同的地方。

知識通常被分為內隱與外顯兩大類：Polanyi(1966)指出「我們所知道的知識遠超過我們所能說的知識」，因為知識分為外顯知識(Tacit Knowledge)：意即可以被具體化、制度化及言語表達的知識；以及內隱知識(Explicit Knowledge)：意即擁有個人特質，與情境相關的，難以具體與表達的知識。

知識依其目的與應用模式及對於現象理解角度的不同，可分為下列幾種類型(Quinn, 1996)：

- Declarative Knowledge: 亦為 Know-what，即了解事物的概念，組成與結構的知識，如學科內容知識，課程知識，學科教學知識等。
- Procedural Knowledge: 亦為 Know-how，即了解事件的執行程序步與方法的知識，如教學程序，教學案例步驟。
- Causal Knowledge: 亦為 Know-why,即了解事件發生的前因後果等關係的知識，如教學程序，教學策略，教學方法之原理。
- Relational Knowledge: 亦為 Know-with，即了解事件與其他因素間關係的知識，如: 學生障礙特質與使用之教學程序，教學策略，教學方法之關係。

2.3.2 Knowledge Creation Process

Nonaka et al. (1994) 認為，知識管理的主要內涵就是知識轉化的過程。存在於個人身上的內隱知識是知識的源頭，是由個人的”潛藏的經驗” (Tacit

Experiences)、構思、洞察力、價值及判斷所組成。它是動態的，而且僅能透過與擁有知識的專家合作及溝通才能存取。因此隱性知識管理除須先將內隱的個體知識團體化(或稱為共同化的過程)，然後再將這種形成團體共識的知識加以外顯化(或稱為外部化的過程)，成為具體明確且可有效使用的組織知識外，同時還需要吸收外部知識使之內部化，以豐富知識存量，然後再將各種不同來源的知識進一步組合化，以增加知識系統對於最終產品與服務的價值(如圖 2.2)。Nonaka 將組織知識創造的過程分成四個模式，分述如下：(Nonaka, 1994)

(1) 共同化(Socialization)

個人不需經由語言便可以得到隱性知識，例如學徒跟著師傅經由觀察、模仿以及練習中學習。但在這樣的簡易的資訊傳遞過程中，雖然只是從腦海中的印象摘要出來，或從共同經驗中體會細微差別的來龍去脈，這已足夠產生某些重要意義。

(2) 外部化(Externalization)

將經驗轉成客觀的顯性知識是很困難的，因為隱性知識很難描述、表達、溝通、並加以形式化；但是我們可以經由隱喻－類比的方法將隱性知識表達出來。

(3) 組合化(Combination)

在這個知識轉換的過程中包括了經由共同化過程將不同個體的顯性知識整合，於其間觀念將逐漸系統化並形成知識體系。例如現代電腦科技的通訊網路與大量資料庫的應用。

(4) 內部化(Internalization)

顯性知識經由不斷的試誤(Trial and Error)實驗，成就了組織的學習並創造了隱性知識(Scott, 1998)。例如以語言、故事或紀錄成文件手冊，都將有助於將顯性知識轉換成隱性知識。在將顯性知識移轉成隱性知識的過程中，活動(Action)占相當重要的角色。

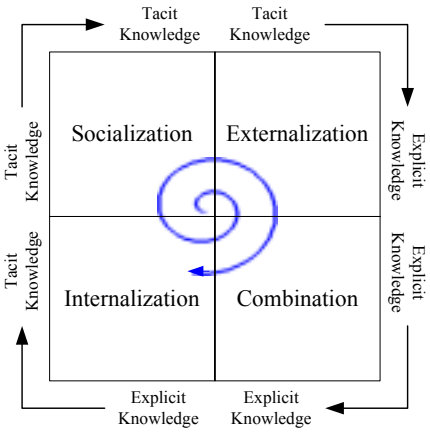


Figure 2.2　Knowledge Creation Process (Nonaka, 1994)

2.3.3 知識管理與其定義

知識管理發展由來已久，依 Macintosh et al.(1999)調查，1975 年 Chaparral Steel 首先採用以知識為焦點的管理訓練課程後，知識管理的歷史便開始演進；1983 年，USAA 發展第一世代的知識庫系統(KBS)，成功地將專家知識移轉給執行者並管理知識(Wiig, 1997)。

知識管理係指組織或個人在面對非連續變化時，將原本存在於組織內知識工作者或隱藏於制度、資料庫、文件、歷史資料之中的知識加以分辨、獲取、選擇、儲存、管理、應用、創造與分享 (Demarest, 1997)；Petrash(1996)將知識管理定義為：把適當的知識(Right Knowledge)在適當的時間(Right Time)給適當的人(Right People)使其做出最佳的決策(Best Decision)；Wiig(1997)指出，知識管理是組織有系統且明確的探索及應用其知識資產(Knowledge Asset)，以提升組織績效，達成報酬最大化；Beckman(1997)認為：知識管理乃是組織利用正式的管道獲取有用的經驗、知識及專業能力，強化組織創新能力並促進對顧客服務的加值；Watson(2003)則認為，知識管理是有計畫的對組織知識資產進行獲取、儲存、檢索、應用、產生與審核(acquisition, storage, retrieval, application, generation,

and review)。

綜上可知，知識管理為一系統化的知識累積過程，藉由強化組織內外部知識的整合，再經由知識分享活動而讓成員取得組織內外部知識、吸收與運用知識，進而發展新知識。如此將使個人或組織皆能因知識的普及而進步，以達成更高的效益。

2.3.4 知識管理策略

目前知識管理的實施以隱性知識管理策略與顯性知識管理策略為主(Coombs and Hull, 1998)，前者旨在將內隱的個體知識團體化(或稱為共同化的過程)，然後再將這種形成團體共識的知識加以外顯化(或稱為外部化的過程)，成為具體明確且可有效使用的組織知識 (Carayannis, 1998)；後者係針對如何取得知識與學習知識，也就是將個人的隱性知識轉化為團體的顯性知識，並增加顯性知識的擴散與流通 (Coombs and Hull, 1998)。茲討論如下：

(1) 隱性知識管理策略：

存在於個人身上的內隱知識是組織知識的源頭，是由個人的『潛藏的經驗』(Tacit Experiences)、構思、洞察力、價值及判斷所組成。它是動態的，而且僅能透過與擁有知識的專家合作及溝通才能存取。因此隱性知識管理除須先將內隱的個體知識團體化(或稱為共同化的過程)，然後再將這種形成團體共識的知識加以外顯化(或稱為外部化的過程)，成為具體明確且可有效使用的組織知識外，同時組織還需要學吸收外部知識使之內部化，以豐富組織的知識存量，然後再將各種不同來源的組織知識進一步組合化，以增加組織知識系統對於最終產品與服務的價值(David, 1996)。隱性知識管理可運用的策略包括：開放性組織知識分享氣息，使不同觀念的人，以交叉影響(cross-pollinating)的方式學習；運用多媒體及網路來增加人際溝通的效率；專案型的團隊管理；良好的教育訓練與學習

機制(Demarest, 1997)等。

(2) 顯性知識管理策略：

顯性知識管理策略主要針對已存在知識的管理，因此重點將放在如何取得知識與學習知識，也就是說如何將個人的隱性知識轉化為團體的顯性知識，並增加顯性知識的擴散與流通。可運用的策略手段包括：有計劃的發展組織知識庫；引進移轉外部知識；設置專責的知識管理部門來從事有關知識的收集、整理、分析與使用；運用網際網路來流通知識、發展標準作業流程、開發專家系統與決策支援系統(Drew, 1999)等。

2.3.5 知識管理程序

Demarest(1997)認為知識管理應分下列五個步驟進行：

(1) 建構(Construction)－經由複雜的步驟(創造、模仿、轉化、重現)產生知識。
(2) 具體化(Embodiment)－將隱性知識轉化成流程、運用方法、機制、與企業文化的一部份。
(3) 擴散(Dissemination)－將具體化的知識傳播到整個企業或價值鏈中。
(4) 使用(Use)－知識的運用。
(5) 管理(Management)－知識經理(在企業中負有促進知識機制運作的責任)必須管理並進行建構、具體化、傳播和使用知識。

Wiig et al. (1997) 則指出：知識管理計畫實行時，會進行下列活動：

(1) 發展(develop)知識：(buy it, learning programs, machine learning on databases)
(2) 傳播(distribute)知識：(to the points of action, KBS's, manuals, network connections
(3) 結合(combine)知識：(find synergies, reuse existing knowledge)

(4) 鞏固(consolidate)知識：(prevent it from disappearing, KBS's, tutoring programs, knowledge transfer programs)

Watson(2003)則將知識管理的活動歸納為下列四者的循環：

(1) 取得知識(acquire knowledge)：如學習、創造、辨識(learn, create, or identify)知識；

(2) 分析知識(analyze knowledge)：如評估、認可、評價(assess, validate, or value)知識；

(3) 保存知識(preserve knowledge)：如組織、表述、維護(organize, represent, or maintain)知識；

(4) 使用知識(use knowledge)： 如應用、轉移、分享(apply, transfer, or share)知識。

綜上，本研究暫將知識管理的程序歸納為知識建構(Construction)、知識萃取(Extraction)、知識整合(Integration)與知識分享(Sharing)等四大步驟的循環，如下圖 2.3。

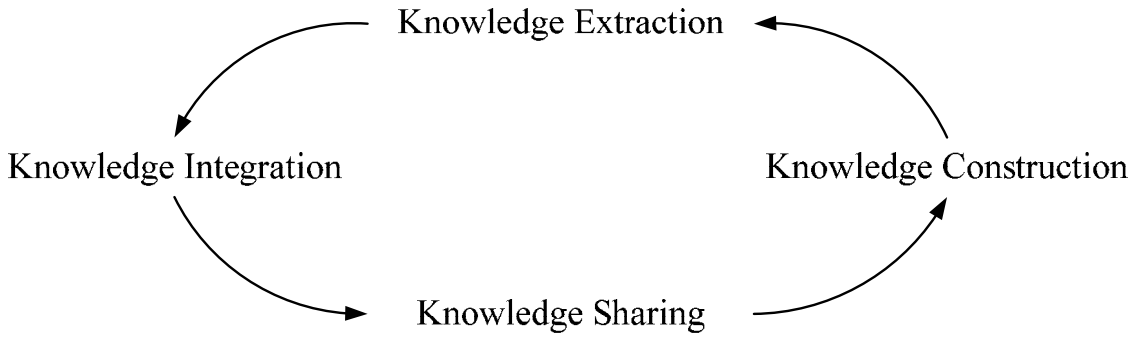


Figure 2.3 知識管理循環

3. KM-based e-Learning Model

3.1 KM-based e-Learning Model

依據前(section 2.1.3)述 Kolb 之經驗學習理論，學習為一種透過經驗轉化而創造知識的過程；經驗學習循環則指學習者(1)直接由體驗中吸收經驗，(2)從經驗中反思體會之後，(3)能將體會的結果一般化(Generalizing)，(4)並應用在一般生活中等四階段的不斷循環。但是，誠如俾斯麥(Otto von Bismarck)所言：『愚者從經驗中學習，我則寧願汲取他人的經驗。』(Fools say they learn by experience, I prefer to profit by others' experience.) (Liddell Hart, 1991)。學習的主要目的之一，就是避免反覆在嘗試錯誤中學習，前章(section 2.1.1)引述學習的定義為「藉由經驗，使行為發生持久性的改變」，其中的經驗，不僅只直接的親身體驗，也包括間接的經驗，如經由閱讀、觀察等方式取得他人的經驗—亦即利用他人的知識，以減少自身反覆嘗試錯誤的次數與風險。故在經驗學習的循環中，有必要加入知識管理的程序，以強調間接經驗在學習過程中的重要性。

另一方面，在知識管理有關知識創造或建構的模式中，大多不強調直接經驗的重要性。所謂”實踐是檢驗真理的唯一標準”，記載在知識庫中的知識，並不盡然能適用於所有使用者，更不能保證其永遠正確—即便該知識被存入知識庫時，已由領域專家審視過亦然；知識庫中的知識傳遞給使用者後，也唯有經由使用者親身體驗，方能確知其是否可行。因此，在知識管理的循環中，有必要加入經驗學習的程序，以強調知識是在直接經驗中所累積精練而成的。

故本研究以 Kolb 之經驗學習循環(Experiential Learning Cycle) (Kolb, 1984)為基礎，結合 2.3.5 節所匯整之知識管理循環，提出一 KM-Based e-Learning Model (如圖 3.1)，並在下節詳述之。

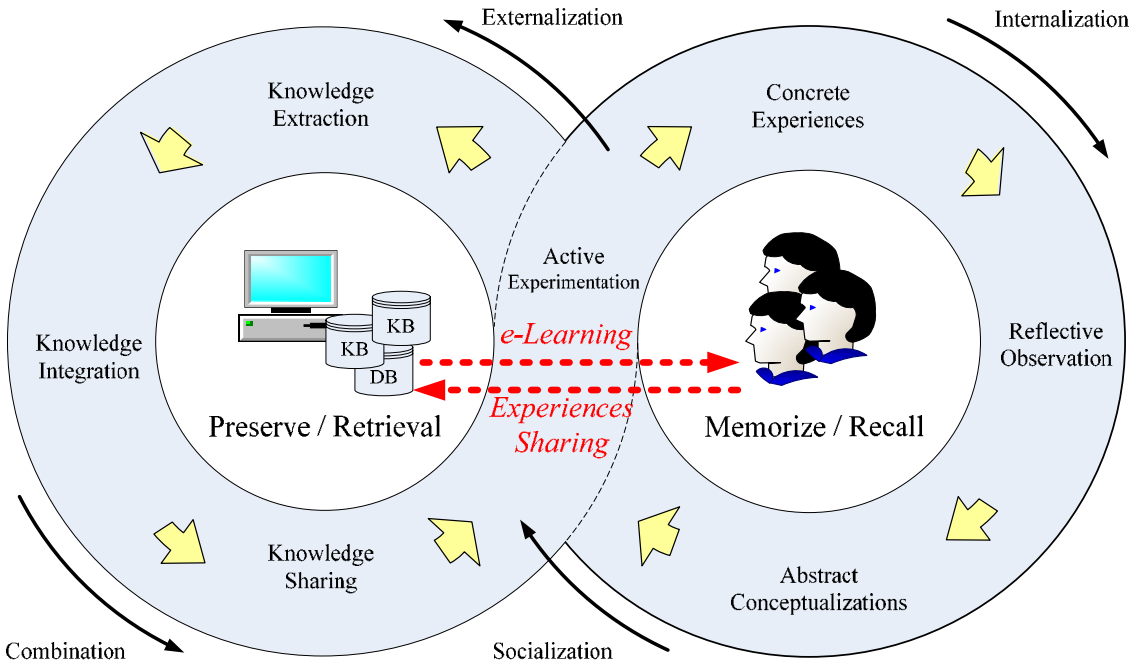


Figure 3.1　KM-Based e-Learning Model

3.2 KM-based e-Learning Model：細部說明

如圖 3.1，Model 由左右兩個循環所組成，其中左半部是 2.3.5 節所匯整之知識管理循環，其中的知識建構(Knowledge Construction)程序被替換為右半部的經驗學習循環——由於經驗學習循環為一透過經驗轉化而創造知識的過程，因此可視為知識建構程序的展開。

在圖 3.1 左半中央有資訊系統(電腦、知識庫、資料庫)，這代表左半的知識管理循環，係以資訊系統為核心，以處理顯性知識為主；進行知識管理循環的程序時，即同時對資訊系統進行保存(Preserve)或檢索(Retrieval)。右半中央有使用者(學習者)，這代表右半的經驗學習循環，係以使用者個人為核心，以處理隱性知識為主；進行經驗學習循環的程序時，即同時對自身(通常是大腦)進行記憶(Memorize)與回憶(Recall)。因此，左半的知識管理循環，可表示前(2.3.4)章所述之顯性知識管理策略；而右半的經驗學習循環，則可表示隱性知識管理策略。

在資訊系統與使用者之間，有虛線箭頭表示兩者間的主要關係：數位學習(e-Learning)與經驗分享(Experiences Sharing)，亦即進行經驗循環時，雖以使用者個人為核心，但仍可透過數位學習取得他人的知識為參考，以減少不必要的嘗試錯誤；而使用者個人也可藉由分享個人經驗，與其他使用者一起互動學習與成長。另，圖中雖未直接表示，在資訊系統的背後，仍需有系統管理員(Administrator)、知識工程師(Knowledge Engineering)、領域專家(Domain Experts)等角色，方能使資訊系統順利運作。

再者，圖 3.1 中；左上半的循環，隱性知識由右側的經驗學習循環中產生，並轉為顯性知識，即為外部化(Externalization)；左下側的循環，顯性知識經過知識整合(Integration)成為另一種形式的顯性知識以利分享，即為組合化(Combination)；右上半的循環中，由左側的知識分享與 e-Learning 中取得顯性知識，再經過個人的實際體驗，轉化為個人的隱性知識，此即為內部化(Internalization)；右下側的循環中，隱性知識在實際體驗中，會成為他人的隱性知識，此即為共同化(Socialization)。因此，過程恰符合 Nonaka 提出之 Knowledge Creation Process (Nonaka, 1994) 四個階段循環，足證本模型符合知識管理之精神。

4. Design of a KM-Based e-Learning Platform

4.1 e-Learning Platform: Overview

數位學習已發展多年，無論是對數位學習理論與系統平台開發皆有相當的進展。在這些研究中發現，數位學習應具備隨時(Any Time)、隨地(Any Where)、方便取得(Easy to Access)等特性，以擺脫傳統教學空間、時間的限制，營造一個自主的、個人的學習空間，並透過網際網路科技互聯成網，使數位教材內容能即時更新、儲存、取用、分配和分享教學或資訊，期能藉由這些特性與資訊科技輔助傳統教學，啟發自主學習意識、提升學習效能。

設計數位學習系統時，需符合學習的精神及特性，否則會偏重系統功能而輕忽學習者需求與教學意義。目前於數位學習平台的相關研究，已有許多研究者針對不同目標及需求提出其學習平台設計，Khan(2005)指出，一個完善數位學習系統需具備 Instructional Design(ID)、Multimedia Component、Internet Tools、Computers and Storage Devices、Connections and Service Providers、Authoring/Management Programs、Enterprise Resource Planning (ERP) Software, and Standards、Server and Related Applications 等元件；此外 Britain and Liber (1999) 學者認為 Virtual Learning Environment 應具有 Notice-board、Course Outline、E-mail Tutor、Conferences、Class list student Home page、Assignments Quizzes、Grade book、Meta data、Synchronous collaboration tools、File upload、Multimedia Resources Repository、Calendar、Search Tools、Book marking、Navigation Model 等功能。

4.2 輕度障礙學生特性

由於數位學習應用層面甚廣，在不同的應用領域(domain)會有不同需求，其功能也各異，需考量各領域特性方能設計出符合需求的功能；本研究係以輕度障礙學生為對象，以下即簡述之。

輕度障礙學生為一特殊群體，在看似正常行為下，卻有學習、表達等障礙，需透過觀察及診斷才能加以判別，並針對其特徵給予適當的輔導。輕度障礙類型大致可分為學習障礙、情緒障礙、輕度智能障礙與高功能自閉症等高發生率障礙群(high incidence disabilities)兒童(Cawley et al., 2003)。這些類型的輕度障礙學生受教權是不該遭受剝奪的，教育體系應針對其障礙類型與特殊需求，給予最適當的輔助。輕度障礙學生在讀、寫、算等基本學習容易感到困難，且在學習過程中普遍有注意力不集中、過動、情緒不穩定等特性，促使學習效果不佳。

Kirk 等學者指出，欲輔導輕度障礙學生，不僅藉由與學生的直接接觸來改變其學習與行為，同時也要改善障礙學生的周遭環境，包括：家庭、學校、社區等整體環境 (Kirk et al., 2003) 。因此，教師需與家長、專家等人合作配搭，方能使輕度障礙學生學習效果得到最大的提升。

4.3 互動分析

在前章所提出的 KM-Based e-Learning Model 中，學習者對一資訊系統進行數位學習，此學習系統在數位學習過程中是相當重要的學習媒介，學習者需利用該系統平台進行學習並與他人分享經驗。在學習過程中，系統會提供相關知識及資源供學習者參考；系統則透過專家持續收集、萃取、審核、建構及維護各種知識與資源，以提供學習者完善的學習經驗。由於功能甚多，本研究將該資訊系統定位為一知識管理為基之數位學習平台(KM-Based e-Learning Platform)，以利整合各功能模組。

規劃設計數位學習平台時，應先考量平台與所有使用者間之互動關係，以了解使用者需求。依據先前分析，本研究將平台使用者分為學習者(Learner，含學生、教師與家長)與專家(Expert，含領域專家與知識工程師)。學習者經由平台獲得知識、資源、解決問題及學習，其中教師與家長則是扮演著監督及輔助學生的角色，在學生學習過程中，可利用平台來觀察或監督學生的學習狀況，以了解學生在學習的過程中是否出現學習障礙，俾給予即時的輔助。

另外，平台內部的專業知識需透過領域專家與知識工程師分工合作，當知識工程師在收集及萃取相關知識及資訊後，再經由領域專家進行知識審核，並將審核過的知識加以建構、儲存及更新。此外領域專家還需針對學習者在學習過程中所提出的問題提供解決方案。以上使用者與平台間之互動關係，本研究彙整於下圖 4.1。

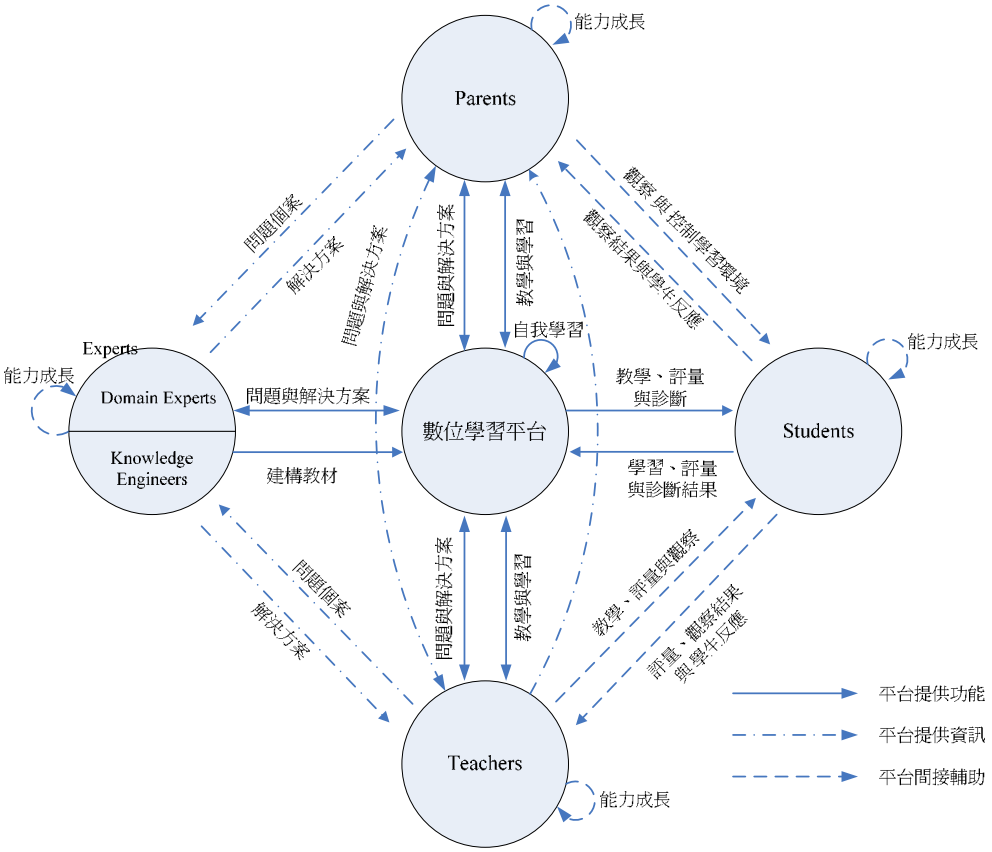


Figure 4.1　e-Learning Platform Interactions

在瞭解使用者與平台間的互動關係後，再參酌前(4.2)節所探討之輕度障礙學生特性與需求，彙整後可推得使用者對數位學習平台之功能需求，如下圖 4.2。

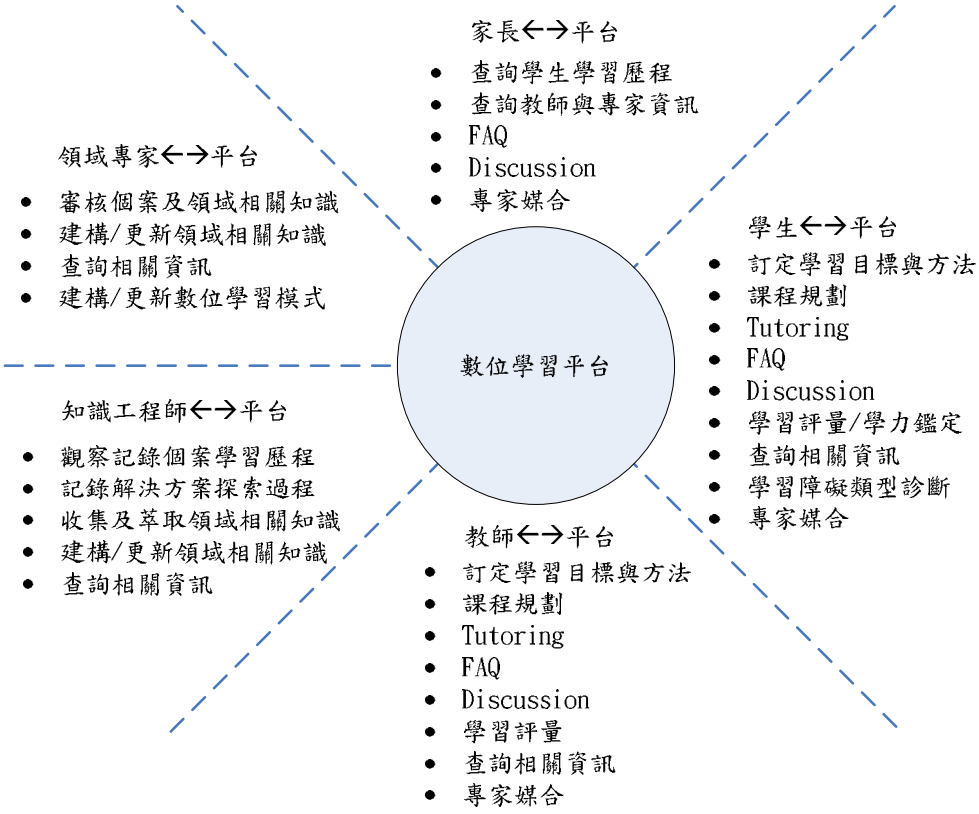


Figure 4.2　功能需求

4.4 功能模組

由圖 4.2 可知，系統平台需提供不同使用者相異的功能，本研究將各功能彙整為六個功能模組，分別為(1)障礙類型診斷、(2)線上教學、(3)常見問題與回應、(4)線上討論區、(5)相關資訊查詢，及(6)知識建構與更新；結果如圖 4.3 所示，其中模組與使用者間的關連性以實線連接表示。各模組功能分述如下：

(1) 障礙類型診斷：針對學生進行初步的障礙類型診斷，依其類別，知會適當的專家給予輔助。

(2) 線上教學：負責訂定、規劃學習目標及學習課程，而學習者則透過該模組進行學習。

(3) 常見問題與回應(FAQ)：當學習者感到疑惑，或在學習過程中遭遇困難時，可透過該模組獲得解答。

(4) 線上討論區：主要是提供學習者在 FAQ 內沒有獲得滿意的答案時，可透過線上討論區向其他學習者或專家尋求解決方案。

(5) 相關資訊查詢：提供使用者查詢相關資訊與領域知識，家長和教師亦可利用該模組查詢到學生整個學習歷程及狀況。

(6) 知識建構與更新：提供領域專家和知識工程師進行應用領域的知識建構，包含審核個案、領域相關知識；觀察紀錄個案的學習歷程及解決方案探索過程；以及收集、萃取、建構與更新領域相關知識等功能。

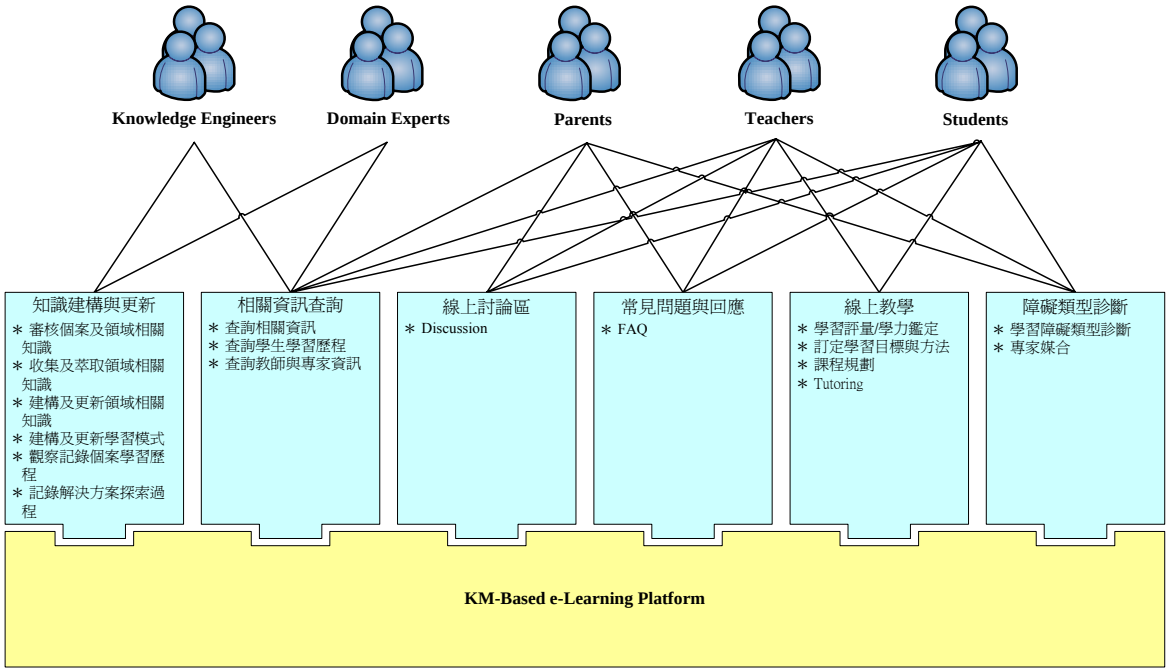


Figure 4.3　功能模組

圖 4.3 所示之數位學習平台功能模組，均屬於提供給使用者的前台功能；而欲維持前台功能運作，則需另由後台模組支援、管理與維護。這些動作需藉助系統管理者(Administrators)與知識工程師的參與，方可順利運作。系統平台的後台依其支援、管理與維護之需求，本研究規劃為四大輔助模組，分別為(1)教材樣版管理、(2)儲存區管理、(3)知識獲取及(4)系統管理，各模組功能說明如下：

(1) 教材樣版管理：該模組主要管理教師在設計教材時所用到的各類樣板。

(2) 儲存區管理：負責管理維護儲存區，並建立儲存區內部的索引檔，以節省系統搜尋資料的時間。

(3) 知識獲取：負責收集及獲取領域知識，並透過系統加以萃取、整合及維護領域的知識。

(4) 系統管理：掌管系統使用者的帳號及權限，並負責維護各項功能模組的安全性，以利系統能順利運作。

4.5 Knowledge Representation Model Design

以輕度障礙學生數學教學為例，教師的知識可分為理論知識與實務知識兩種，故本研究將知識的範疇分成理論知識與實務知識兩層，前者包括概念與相關教材，後者包括各種個案及與個案相關之教學程序，教學策略與教學方法。綜上，本研究即依此設計知識儲存區架構如圖 4.4。

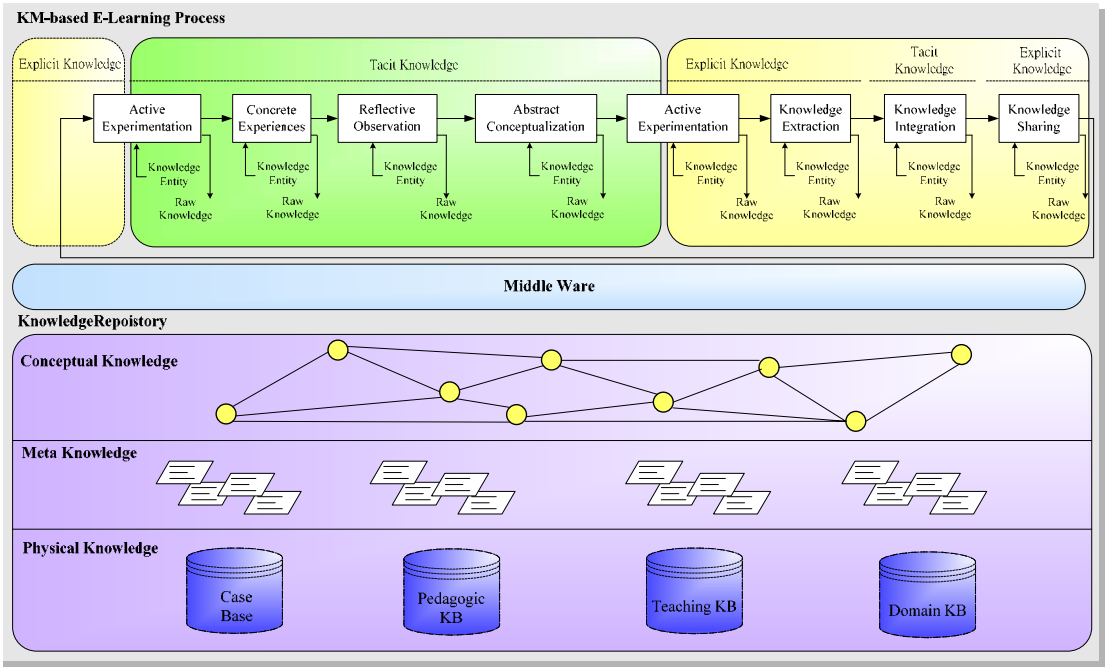


Figure 4.4　Knowledge Repository Framework

4.6　KM-Based e-Learning Platform Functional Framework Design

如 4.4 節所述，數位學習平台包含前台的功能模組和後台的管理模組。在後

台的儲存區部份，本研究將其劃分為資料庫(Database)與知識儲存區(Knowledge Repository)兩種：資料庫存放系統管理相關的資料（如：使用者基本資料、記錄檔等）並利用已成熟的資料庫管理系統(DBMS)來管理；而知識儲存區則存放應用領域相關知識（如個案、教學知識等），其內容則依圖 4.4 知識儲存區架構進行規劃，以提供各類知識庫運作，並以知識管理引擎作為平台與知識儲存區間的運作媒介。

綜上，本研究設計一 KM-Based e-Learning Platform Functional Framework，如圖 4.5。

5. Conclusion

本研究提出一 KM-based e-Learning Model，並依據此設計建構 e-Learning Platform，使該平台具備知識擷取、存取、管理、分享與學習等功能及機制，以進行知識存取及管理時更加正確與便捷，且提供使用者一個良好的數位學習環境，進而實現數位學習之目標與價值。

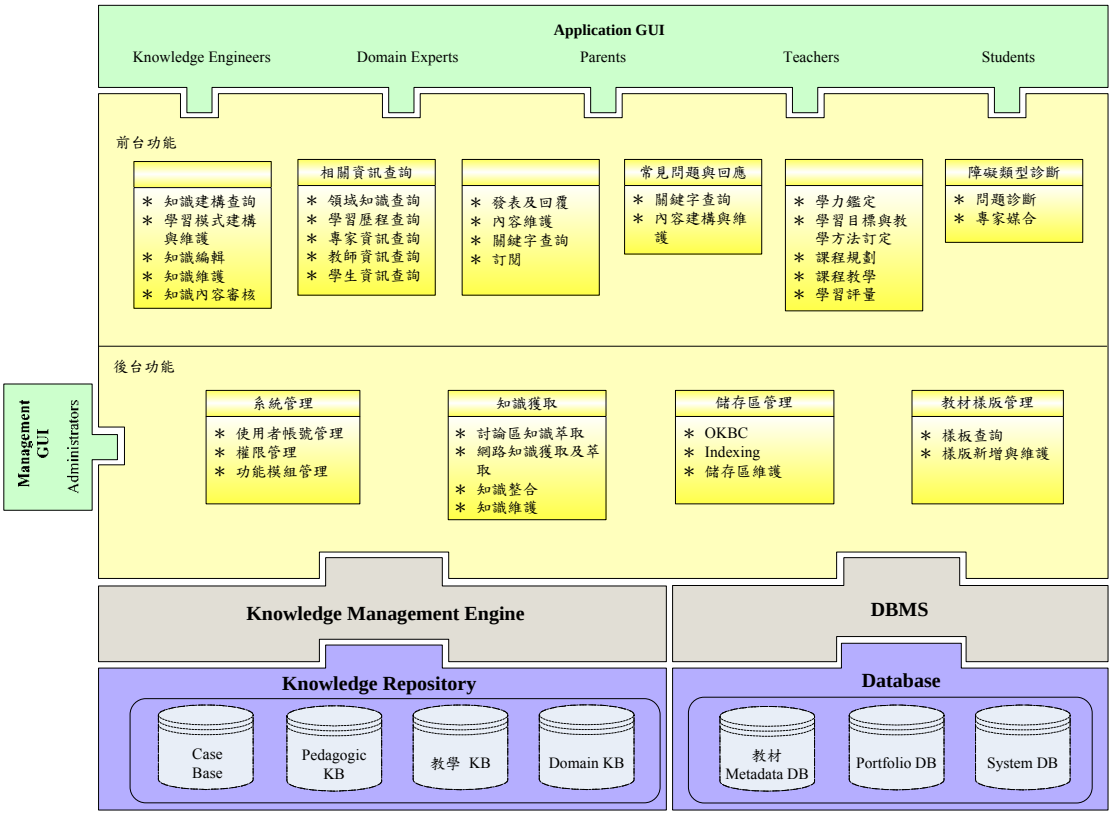


Figure 4.5　KM-Based e-Learning Platform Functional Framework

Reference

1. Hwang, G. J., A tutoring strategy supporting system for distance learning on computer networks. IEEE Transactions on Education, Vol. 41, No. 4, pp. 343-343., 1998
2. Sun, C. T. & C. Chou, Experiencing CORAL: design and implementation of distance cooperative learning. IEEE Transactions on Education, Vol. 39, No. 3, pp. 357-366., 1996
3. Rosenberg Marc J., E-Learning: Strategies for Delivering Knowledge in the Digital Age. McGraw-Hill, 2001
4. Urdan, T. & C. Weggen, Corporate e-Learning: Exploring a New Frontier March 2000. A Research Paper from WR Hambrecht & Co, available on line at http://www.wrhambrecht.com/research/coverage/elearning/
5. Demarest, M., Understanding Knowledge Management. Long Range Planning, Vol: 30, Issue: 3 , pp. 321-322,374-384, 1997
6. Kolb, D. A., Experiential learning: Experience as the source of learning and development. Englewood Cliffs, NJ: Prentice Hall, 1984
7. Nonaka, I. & H. Takeuchi, The Knowledge Creating Company. New York: Oxford University Press, 1995
8. Quinn, J., & P. Anderson, & S. Finkelstein, Managing Professional Intellect: Making the most of the best. Harvard Business Review, 1996
9. Liddell Hart, B. H., Strategy: Second Revised Edition, Plume, 1991
10. Lammari, N., E. Métais, Building and maintaining ontologies: a set of algorithms. Data &. Knowledge Engineering 48, pp. 155–176, 2004
11. Coombs, R., R. Hull, Knowledge management practices and path-dependency in innovation. Research Policy, Vol: 27, Issue: 3 , pp. 237-253, 1998
12. Carayannis, E. G., The strategic management of technological learning in project / program management: the role of extranets, intranets and intelligent agents in knowledge generation, diffusion, and leveraging, Technovation. Vol: 18, Issue: 11 , pp. 697-703, 1998
13. Demarest, M., Understanding Knowledge Management, Long Range Planning, Vol: 30, Issue: 3, pp. 321-322,374-384, 1997
14. Drew, S., Building Knowledge Management into Strategy: Making Sense of a New Perspective. Long Range Planning, Vol: 32, pp130-136, March 1999
15. Wiig, K. M., and d. H. Robert, and V. D. S. Rob, Supporting knowledge management: A selection of methods and techniques, Expert System with Application. Vol.13, No.1, pp.15-27, 1997

16. Nonaka, I., A Dynamic theory of organizational knowledge creation. Organization Science, Vol.5, No.1, 1994
17. Machlup, F., Semantic quirks in studies of information. In: F. Machlup and U. Mansfield, editors, The study of information. New York: John Wiley, 1983
18. Scott, J. E., Organization knowledge and the Intranet. Decision Support System, 23, pp.3-17, 1998
19. Polanyi, M., The Tacit Dimension. London: Routledge & Kegan Paul, 1966
20. Macintosh, A., and F. Ian, and K. John, Knowledge management techniques: teaching and dissemination concepts. Int. J. Human-Computer Studies, Vol.51, pp.549-566, 1999
21. Beckman, T. J., A Methodology for Knowledge Management. International Association of Science and Technology for Development (IASTED) AI and Soft Computing Conference, Banff, Canada, 1997
22. Petrash, G., Managing Knowledge Assets for Value. Knowledge-Based Leadership Conference, Boston: Linkage Inc., 1996
23. Weiss, H. M., Learning theory and industrial and organizational psychology. In: M. D. Dunnette, L. M. Hough, editors. Handbook of industrial and organizational psychology. 2nd ed. Vol. 1, Palo Alto, CA: Consulting Psychological Press, pp.172-173, 1990
24. Robbins, S. P., Organizational Behavior. 9th ed. Prentice Hall, 2001
25. David, P.; Sharpe, S. Human-Centered Knowledge Acquisition: a structural learning theory approach. Int. J. Human Computer studies, Vol: 45, pp381-396, 1996
26. Henderson, A. J., The E-Learning Question and Answer Book: A Survival Guide for Trainers and Business Managers. AMACOM, 2003
27. Watson, I., Applying Knowledge Management: Techniques for Building Corporate Memories. Morgan Kaufmann Publishers, 2003
28. Bergeron, B., Essentials of Knowledge Management. John Wiley & Sons Ltd., page 4, 2003
29. Bonk, C. J., R. A. Wisher, J. Y. Lee, Moderating Learner-Centered E-Learning: Problems and Solutions, Benefits and Implications. In: T. S. Roberts editor, Online Collaborative Learning: Theory and Practice. Information Science Publishing, 2004
30. Morrison, D., E-learning Strategies: How to get implementation and delivery right first time. John Wiley & Sons Ltd., 2003
31. Huerta, E., T. Ryan, M. Igbaria, A Comprehensive Web-Based Learning Framework: Toward Theoretical Diversity. In: A. K. Aggarwal editor, Web-Based Education: Learning from Experience. IRM Press, 2003

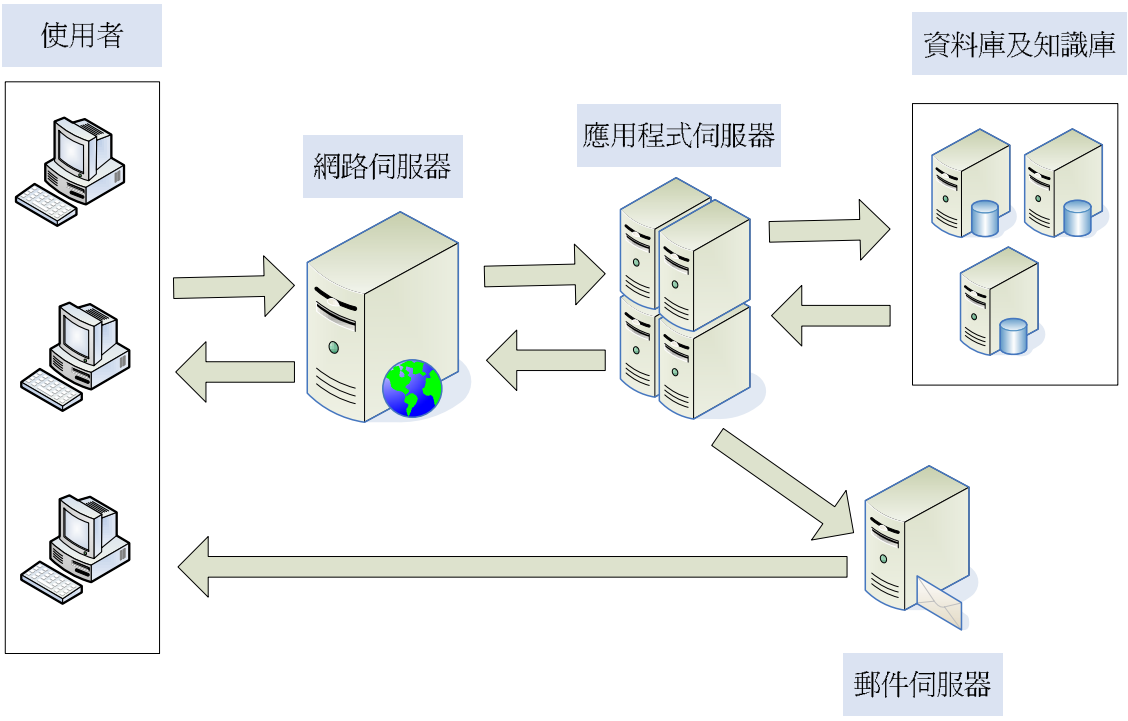
32. Cawley, J. F., T. E. Foley, J. Miller, Science and Students with Mild Disabilities. Intervention in School & Clinic, 38, 153-189, 2003
33. Kirk, S. A., J. J. Gallagher, N. T. Anastasiow, Educating exceptional children. 10th ed., Boston：Houghton Miffin Company, 2003
34. 張春興、林清山, 教育心理學. 台北：東華, 1996
35. Antal, P., Animated explanations using adaptive student models. Proc. of INES'97, pp. 573-576, 1997
36. Principle, J. C., N. Euliano, and C. Lefebvre, An interactive learning environment for adaptive systems instruction. Proc. of the 1998 IEEE Int'l Conf. on Acoustics, Speech and Signal Processing, Vol. 3, pp. 1901-1904, 1998
37. Urdan, T. & C. Weggen, Corporate e-Learning: Exploring a New Frontier. March 2000. A Research Paper from WR Hambrecht & Co, available online at http://www.wrhambrecht.com/research/coverage/elearning/, 23 July, 2000
38. 蔡昌均、曾憲雄、林智揚(民 91)：中文化 e-learning 共享教材元件標準之規範，資訊與教育第八十九期。
39. 朱治平、張慶寶、葉瓊韋(民 92)：基於 Web Service 技術之學習管理系統。中華民國自動化科技學會會刊。
40. SCORM(Sharable Content Object Reference Model), hhttp://www.adlnet.org/
41. LTSC(IEEE Learning Technology Standards Committee), http://ltsc.ieee.org/wg12
42. LMML(Learning Material Markup Language), http://www.lmml.de
43. Britain, S., & Liber, O. (1999). A framework for pedagogical evaluation of virtual learning environments. University of Wales-Bangor, JSC TAP report 41; http://www.jtap.ac.uk/reports/htmal/jtap-041.html.

附件(二) 數位學習平台整體架構之設計

一、 數位學習平台之系統配置

本系統配置將區分為使用者端、網路應用伺服器、應用程式伺服器、資料庫

及知識庫、郵件伺服器，如圖一所示。網路伺服器：主要提供本系統主要網頁介面給使用者進行連結及使用相關系統功能；應用程式伺服器：主要提供本系統相關系統功能程式的儲存，將本系統所有的應用程式儲存於此，當使用者進行使用本系統時，系統將會連結至此伺服器進行應用程式的運算，再將最終結果回覆至網路頁面上；資料庫及知識庫：主要提供本系統相關資料及知識的儲存；郵件伺服器：主要提供本系統進行郵件的傳送。



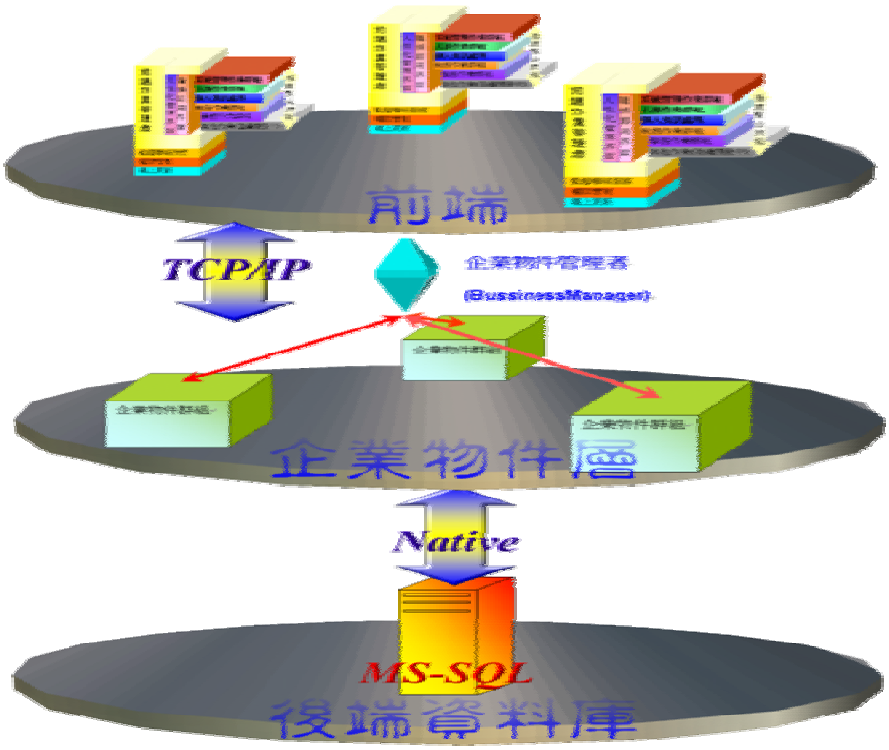
圖一　數位學習平台之系統配置圖

二、 系統開發環境與平台

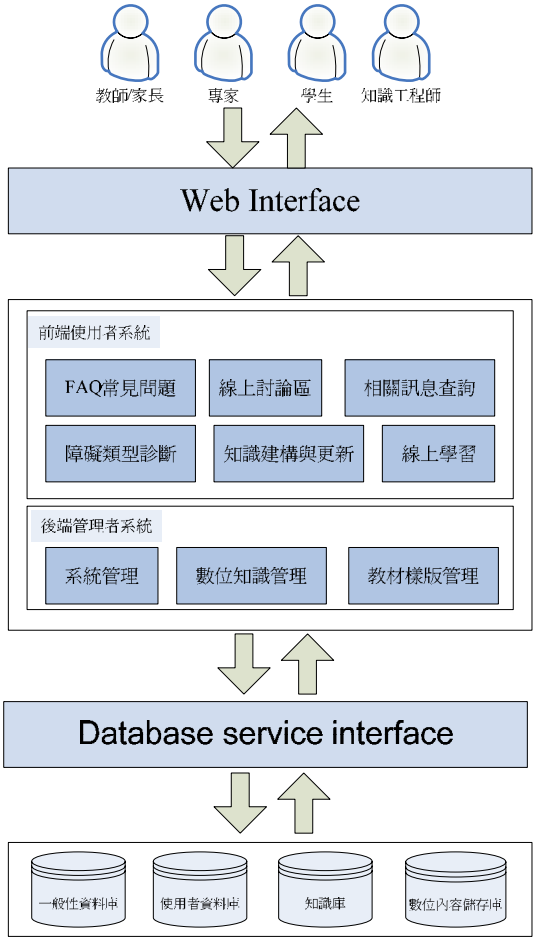
1. 伺服器軟體：
   DB : MS SQL Server 2000。
   WEB: Apache Tomcat Server。
   Java 2SE 5.0。
   Application Server: 採用自行研發之分散式企業物件模型。。
2. 開發工具：
   JBuilder 2006。
3. 作業系統
   Server: Windows 2000。
   Client: Windows 95/98/XP。
4. 使用者介面： Web Form 整合作業。

三、 數位學習平台之系統架構

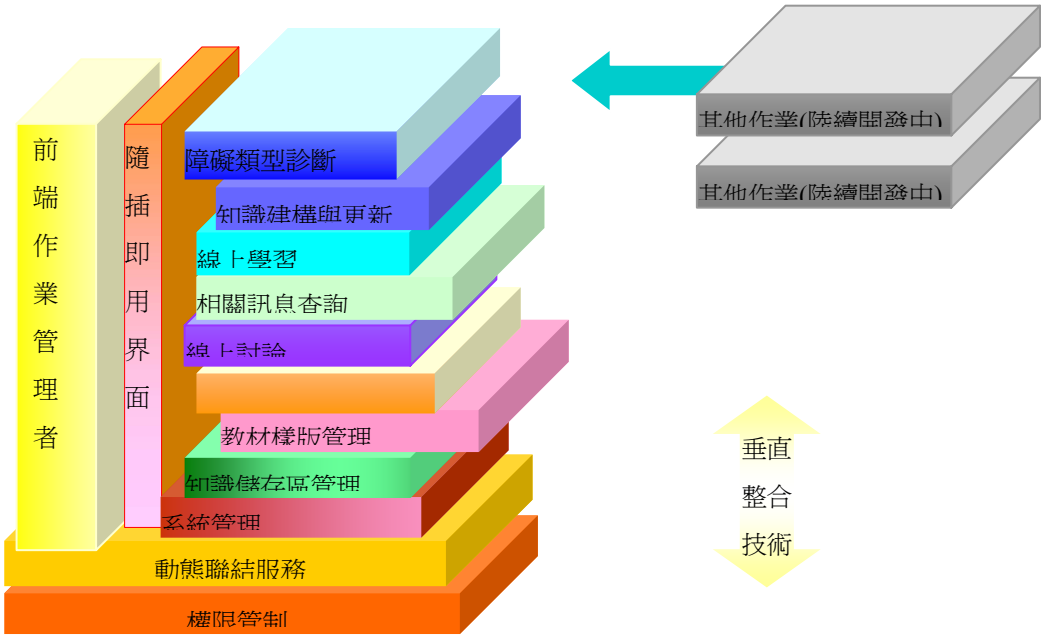
本系統規劃採用多層次(Multi-Tier)&分散式物件(Distributed Objects)資訊處理架構並以循環式動態性整合的系統發展模型建構，如圖二所示。運用類似網路服務(Web service)的概念將本系統各功能拆解成各個獨立的服務提供者，當應用程式或使用者進行系統使應用時，各應用程式便可提供與需求相對應的應用服務，最後再將結果傳回給要求服務的應用程式或使用者，系統架構圖如圖三所示。此模式能方便系統的同步開發及系統效率的調整，當開發出效率更好的應用程式時便能將原有的應用程式直接抽換成新的應用程式，省去更動程式內容時所要負擔的風險。而在系統開發時也可將各逐步完成的功能附掛置系統上，加快系統開發人員在進行系統開發時的開發效率，因此本平台可以分為前端作業管理平台與企業物件層架構，如圖四、圖五。



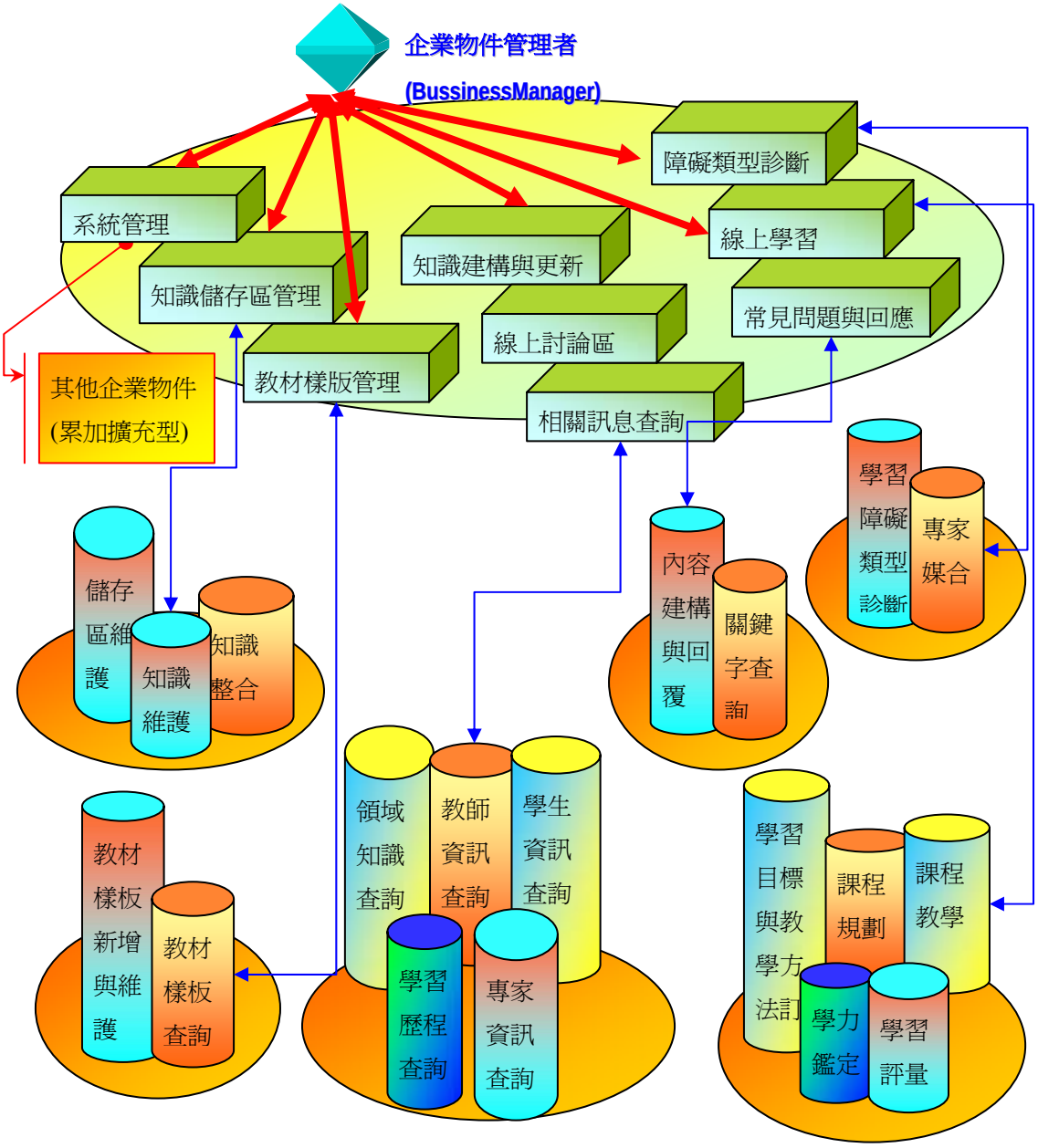
圖二 多層次與分散式物件之資訊處理架構



圖三 數位學習平台之系統架構圖



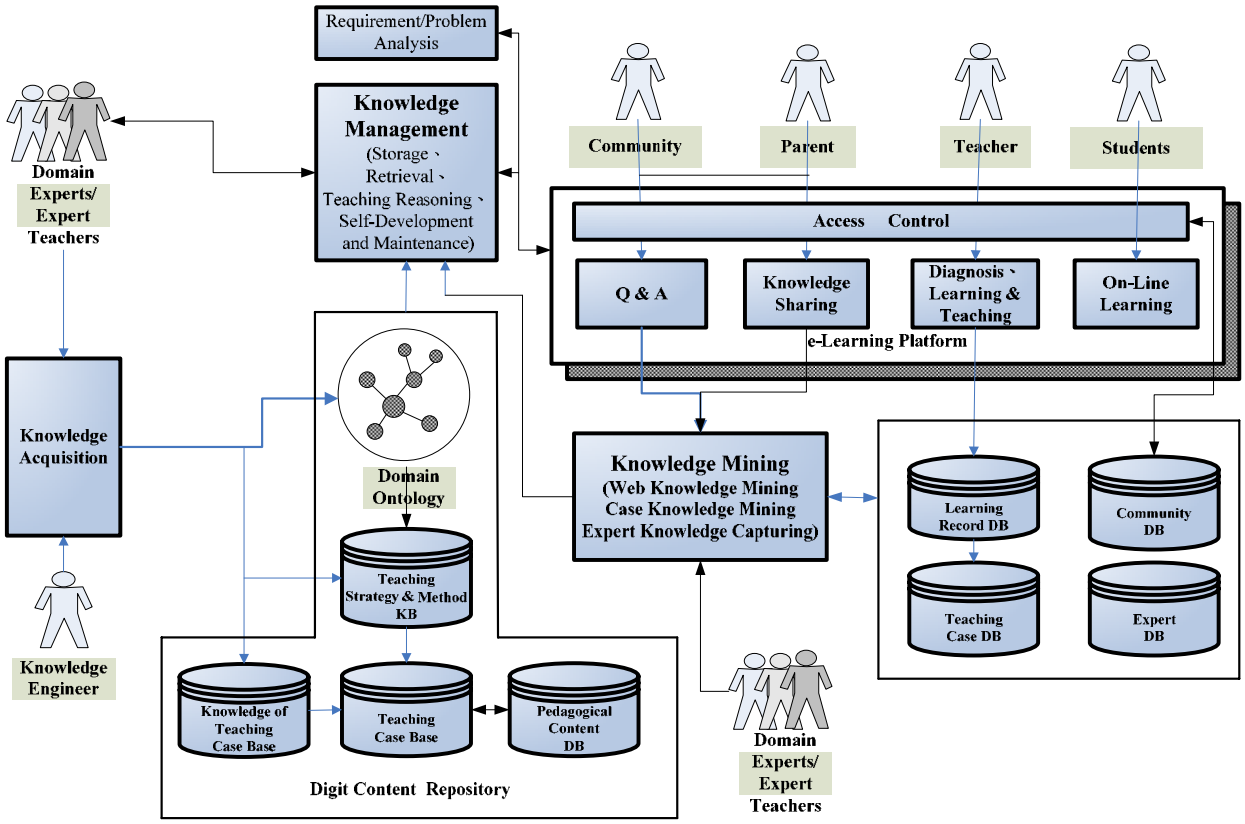
圖四 前端作業管理平台



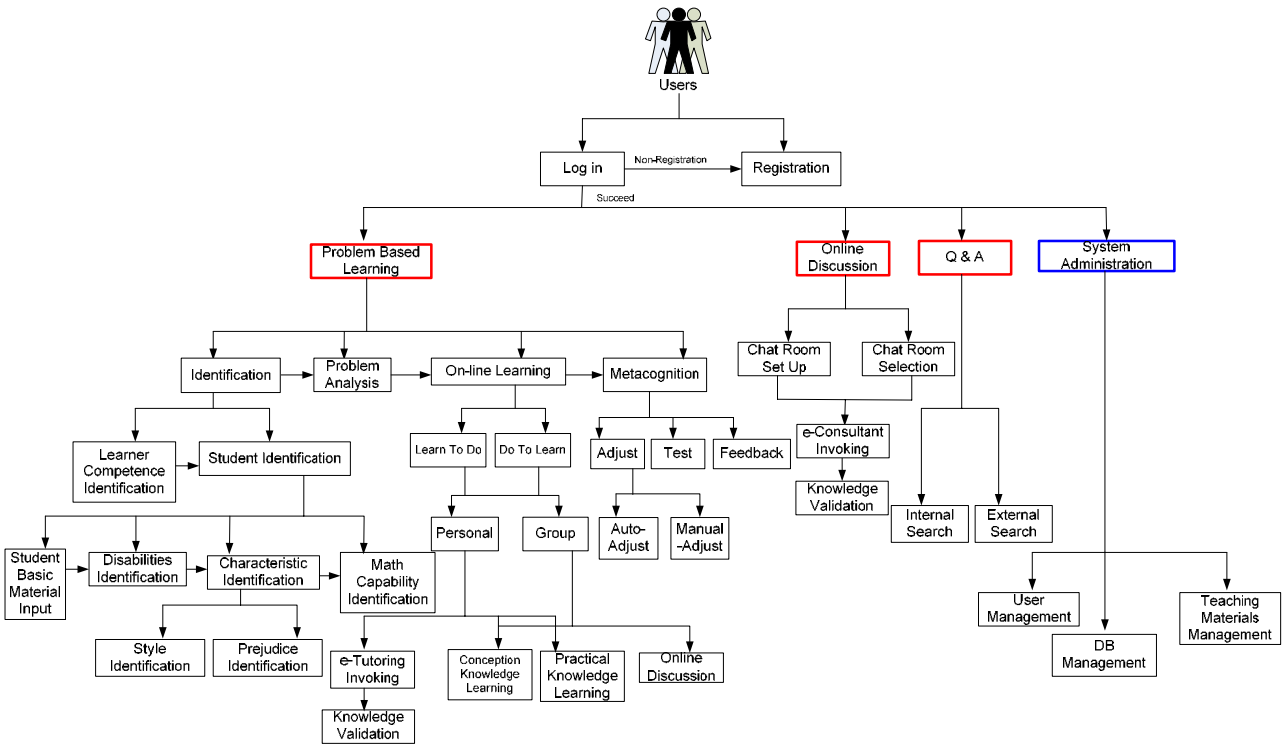
圖五 企業物件層架構圖

四、 數位學習平台功能架構之設計

本平台之主要功能模組如圖六所示，包括:功能介面、核心模組、知識管理引擎、數位知識內容儲存區四層；功能介面包括: 個案診斷教學、知識分享、問題詢答、受輔學生線上學習、專家庫與社群及系統管理；知識管理實現元件包括: 知識儲存、知識撿索、個案診斷教學推理、系統自我學習與內容維護；數位內容儲存區將儲存之數位內容包括: 數位知識、教學案例及個案診斷與學習歷程資料，平台之細部功能架構，如圖七。



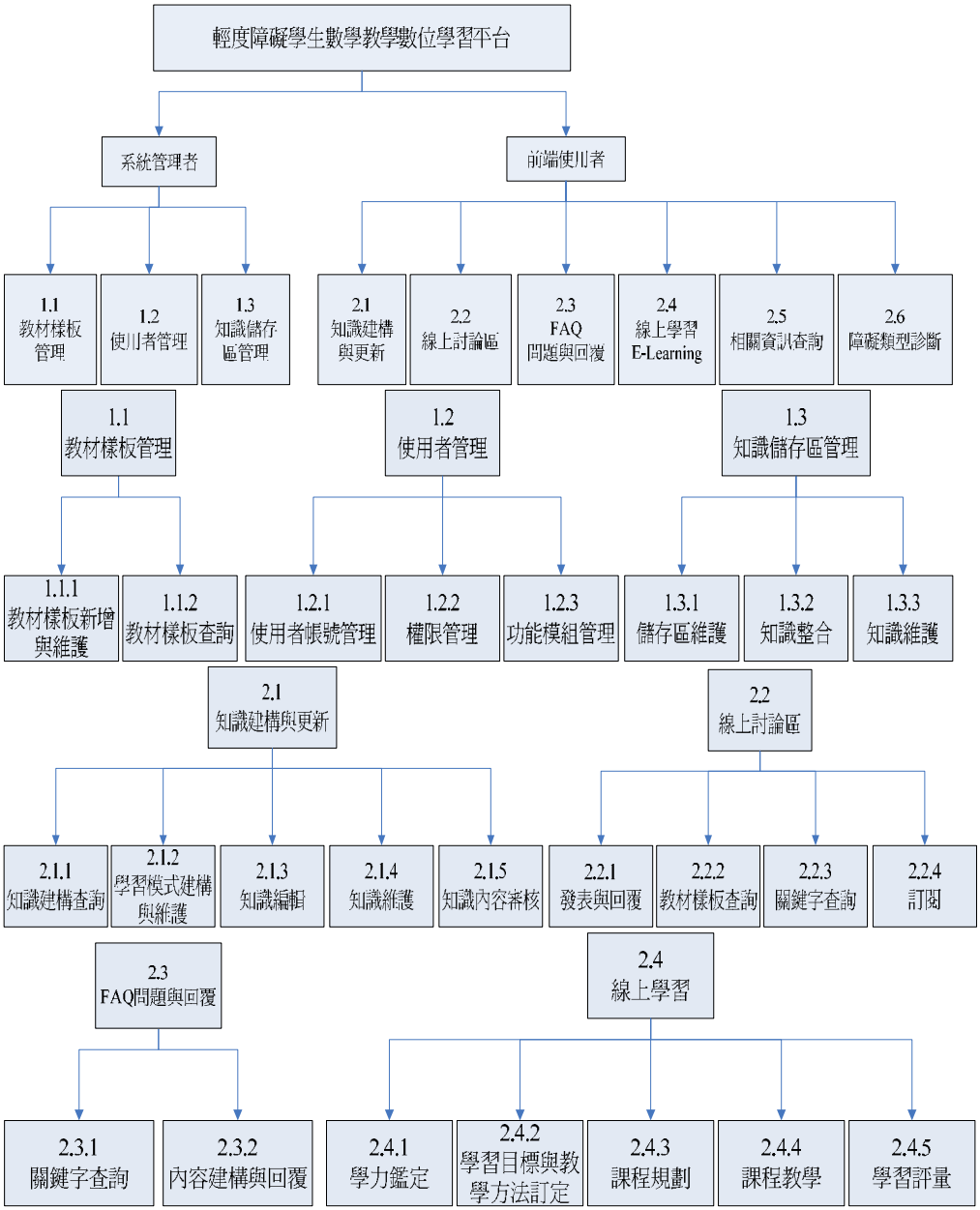
圖六 數位學習平台系統之主要功能模組

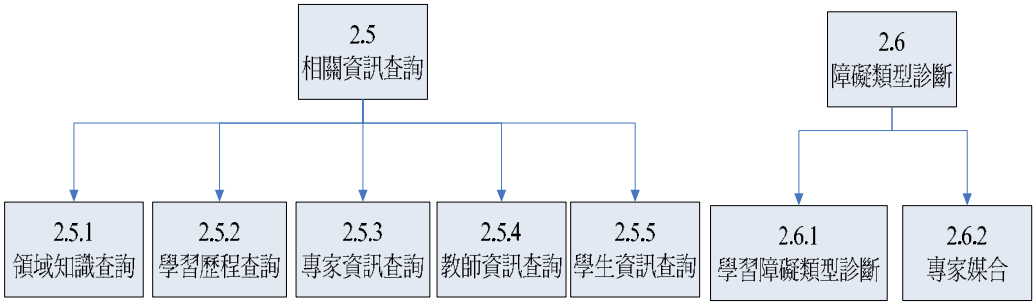


圖七 數位學習平台系統之細部功能架構

五、 數位學習平台功能模組之使用者介面設計

本數位學習平台使用者介面之設計圖，如圖八所示，使用者對象可分為系統管理者與前端使用者，平台提供給管理者「教材樣版管理」、「使用者管理」與「知識儲存管理」；另平台可以讓使用者進行「線上學習」，並提供「線上討論區」、「FAQ問題與回覆」、「相關資訊查詢」、「知識確認」之功能，詳細內容分述如下：





圖八 數位學習平台使用者介面之設計圖

1.1 教材樣版管理

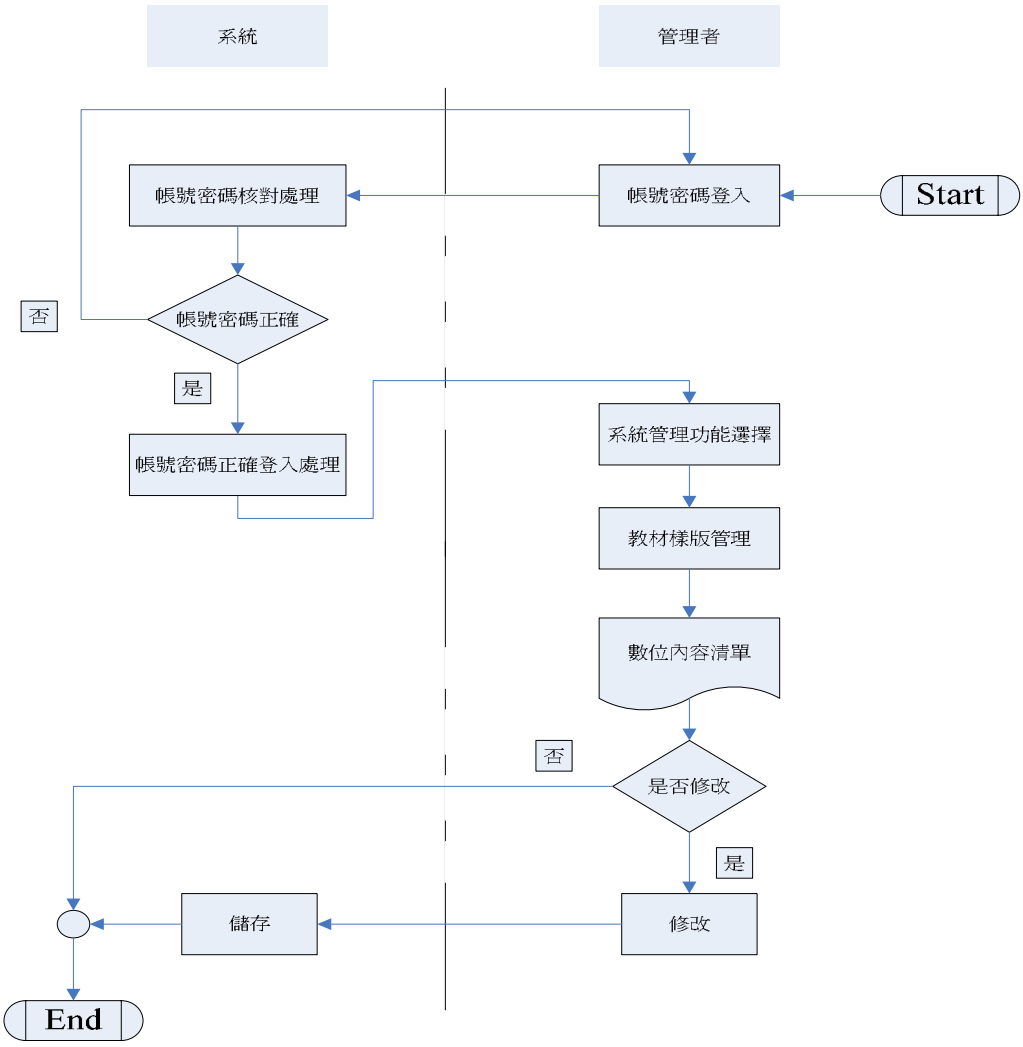
管理者登入系統後選擇教材樣板功能，選擇後系統會列出教材樣版資料清單，管理者可就既有的資料進行修正或刪除，也可新增教材樣版資料。

1.2 使用者管理

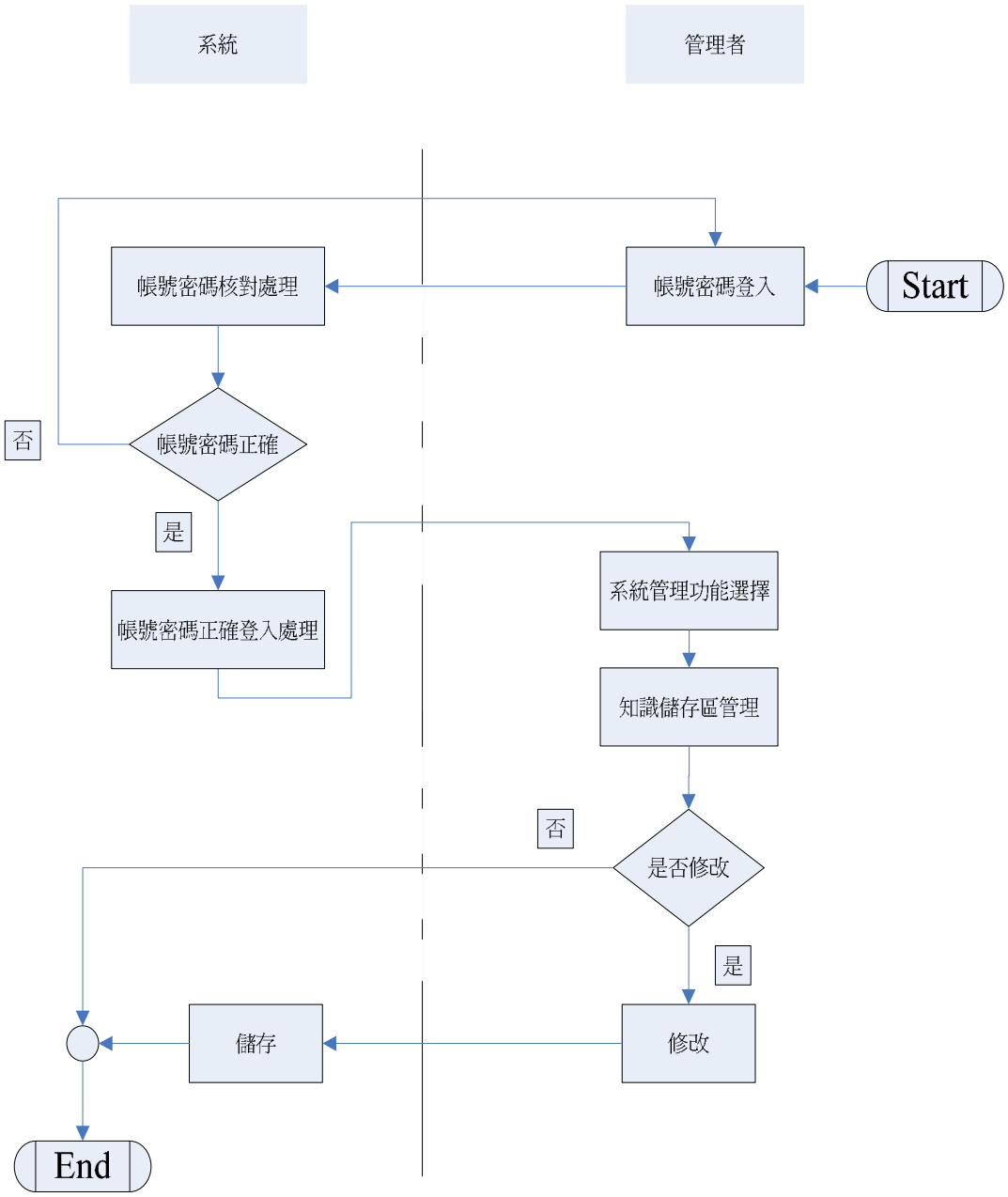
管理者登入系統後選擇使用者帳號管理功能，選擇後系統會列出使用者帳號資料清單，管理者可就原有的資料進行修正或刪除。

1.3 知識儲存區管理

管理者登入系統後選擇知識儲存區管理功能，選擇後系統便列出相關知識庫內容，管理者可就知識儲存區內資料進行修正。



圖九 教材樣版、使用者管理流程圖

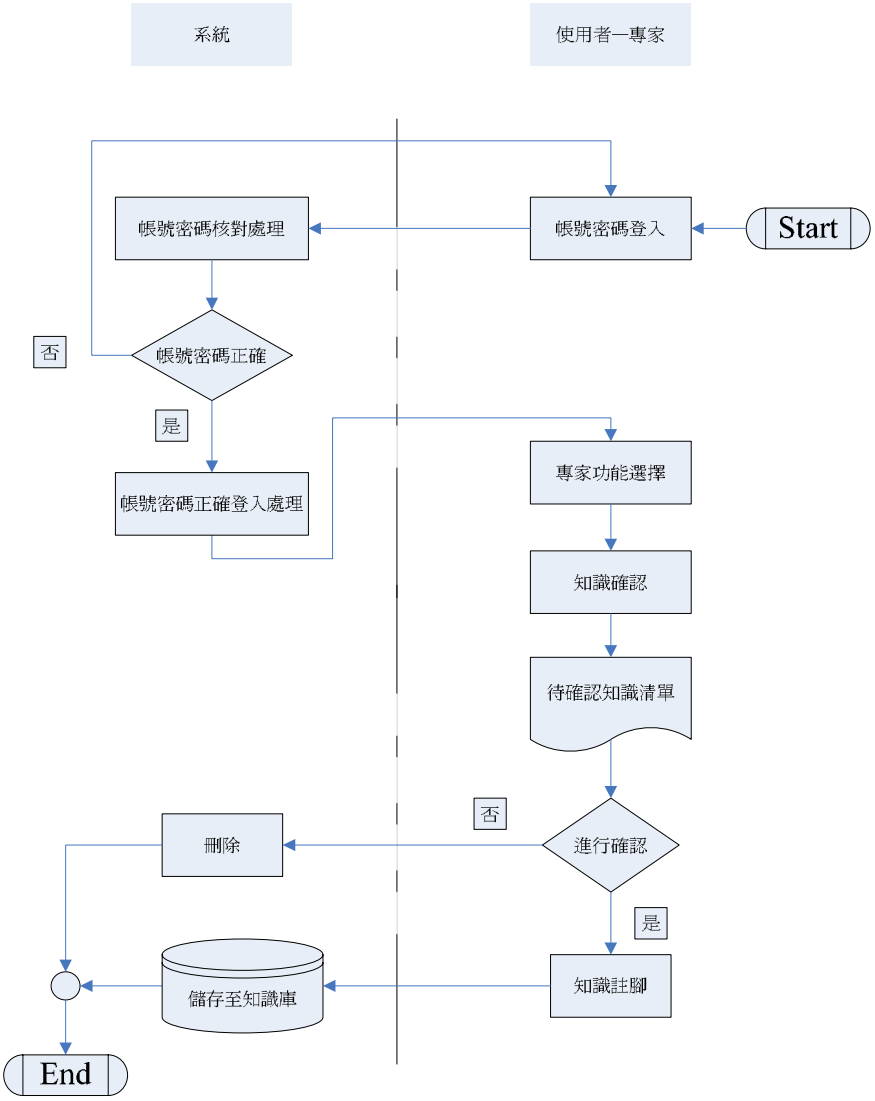


圖十 知識儲存區管理流程圖

2.1 知識確認

專家使用者登入系統後選擇知識確認功能，選擇後系統便列出相關待審

之知識清單內容，專家使用者可就待審知識資料進行確認審核及加入註解，金行知識的篩選。



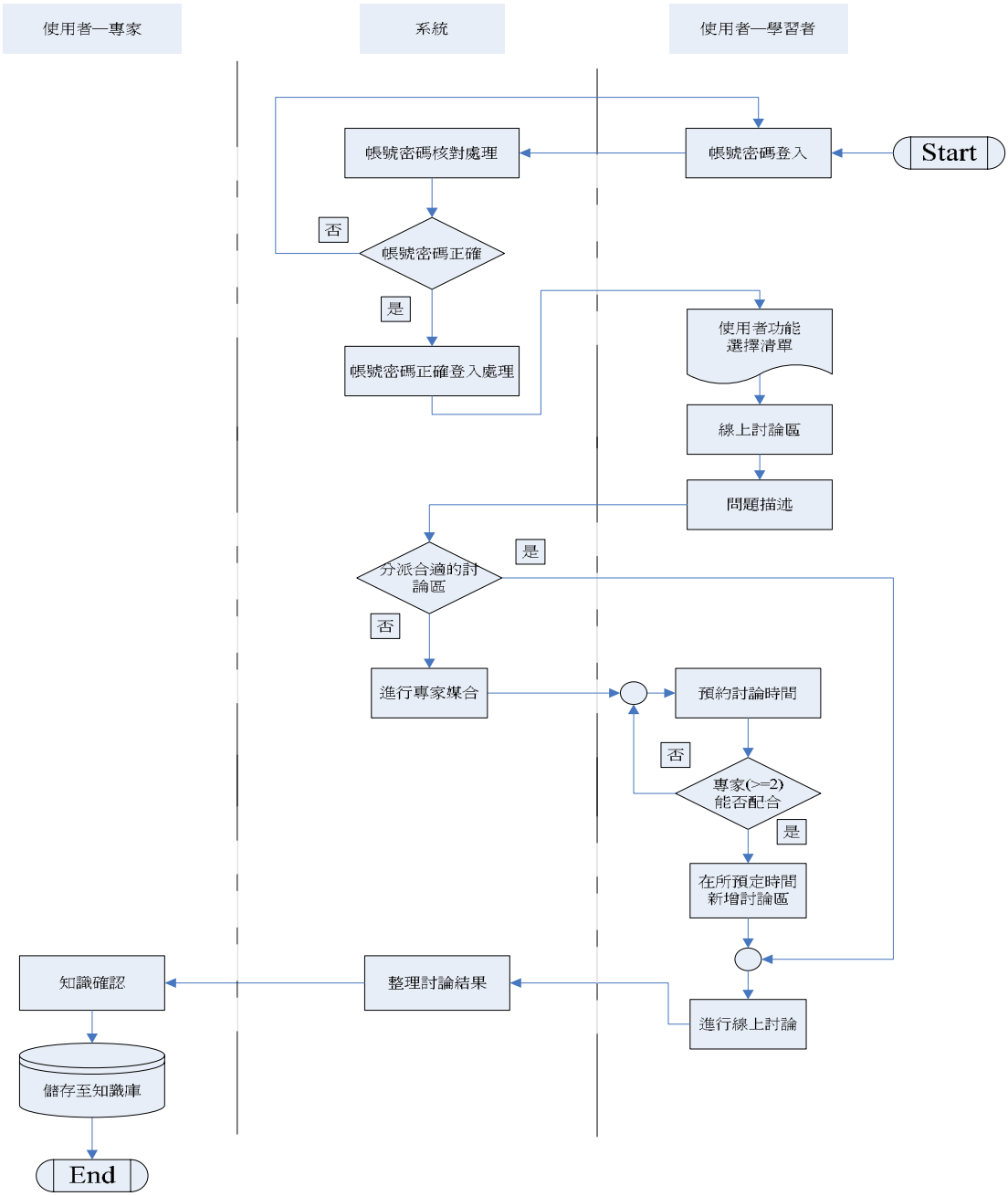
圖十一 知識確認流程圖

2.2 線上討論區

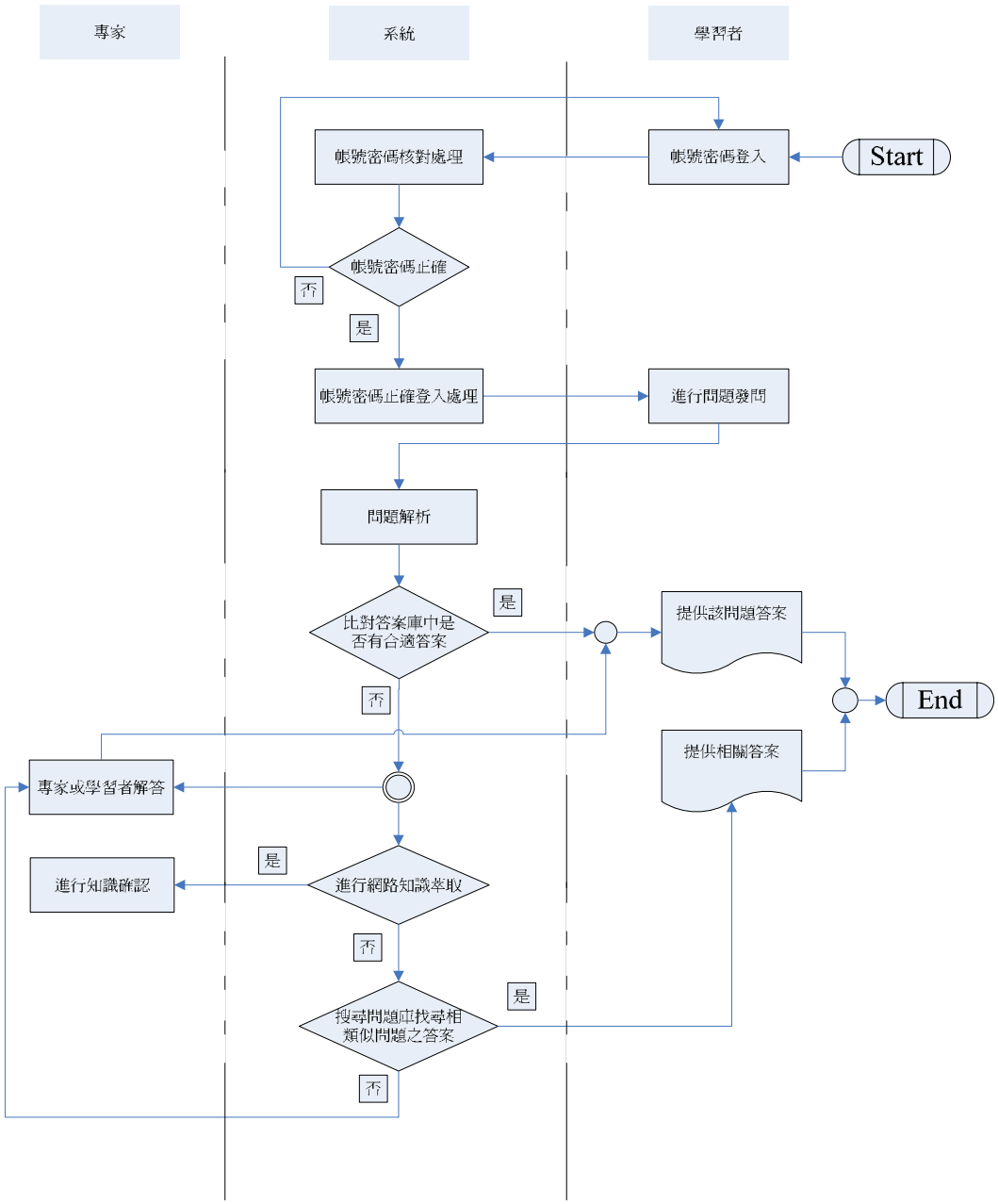
使用者欲進行線上討論時，使用者需將欲討論問題輸入至頁面透過系統對問題的拆解處理，將使用者分派至合適該問題的相關討論區中，如果使用者覺得不符合討論議題則可以另外預約一討論區，系統將會真對使用者的問題與領域專家進行配對，找出合適的領域專家，並預約雙方合適的時間再進行線上討論，系統並將討論結果進行節錄篩選，將這些知識經由領域專家的確認儲存至知識庫中。

2.3FAQ 問題與回覆

使用者至本系統進行相關問題的發問，系統會真對使用者的問題進行拆解並比對答案庫中是否有合適的資料，有合適的資料則直接回覆至頁面。如果搜尋不到資料則啟動網路搜尋機制，至網路上搜尋與問題相關的資訊加以整理過後再將答案回覆給使用者。如果回覆的資訊無法滿足使用者的需求，則系統會將問題儲存於暫存區中等待專家或是其他學習者的回覆。



圖十二 線上討論區流程圖



圖十三 FAQ 問題與回覆流程圖

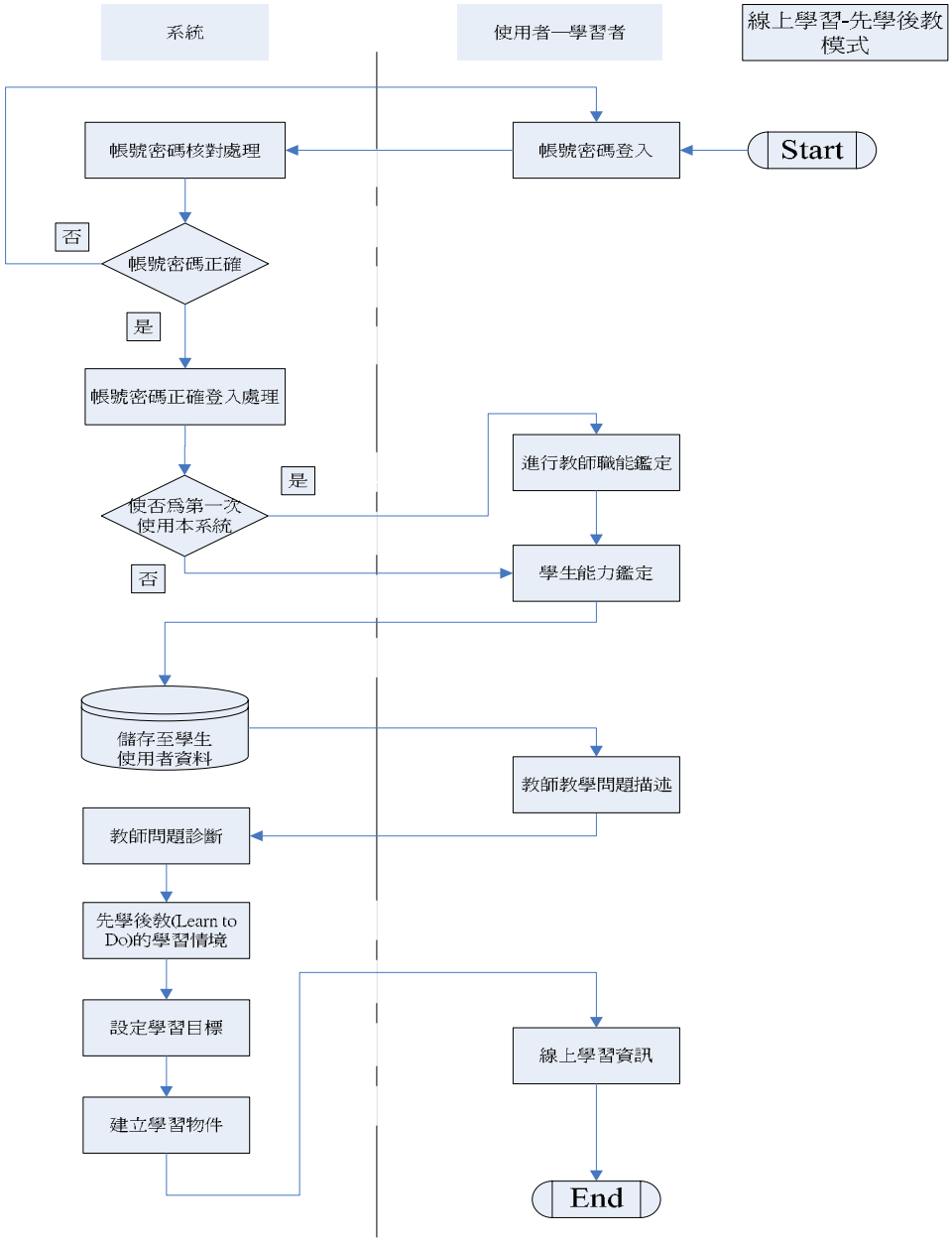
2.4 線上學習

線上學習主要分成 1..先學後教、2.邊學邊教兩種學習模式。在進行線

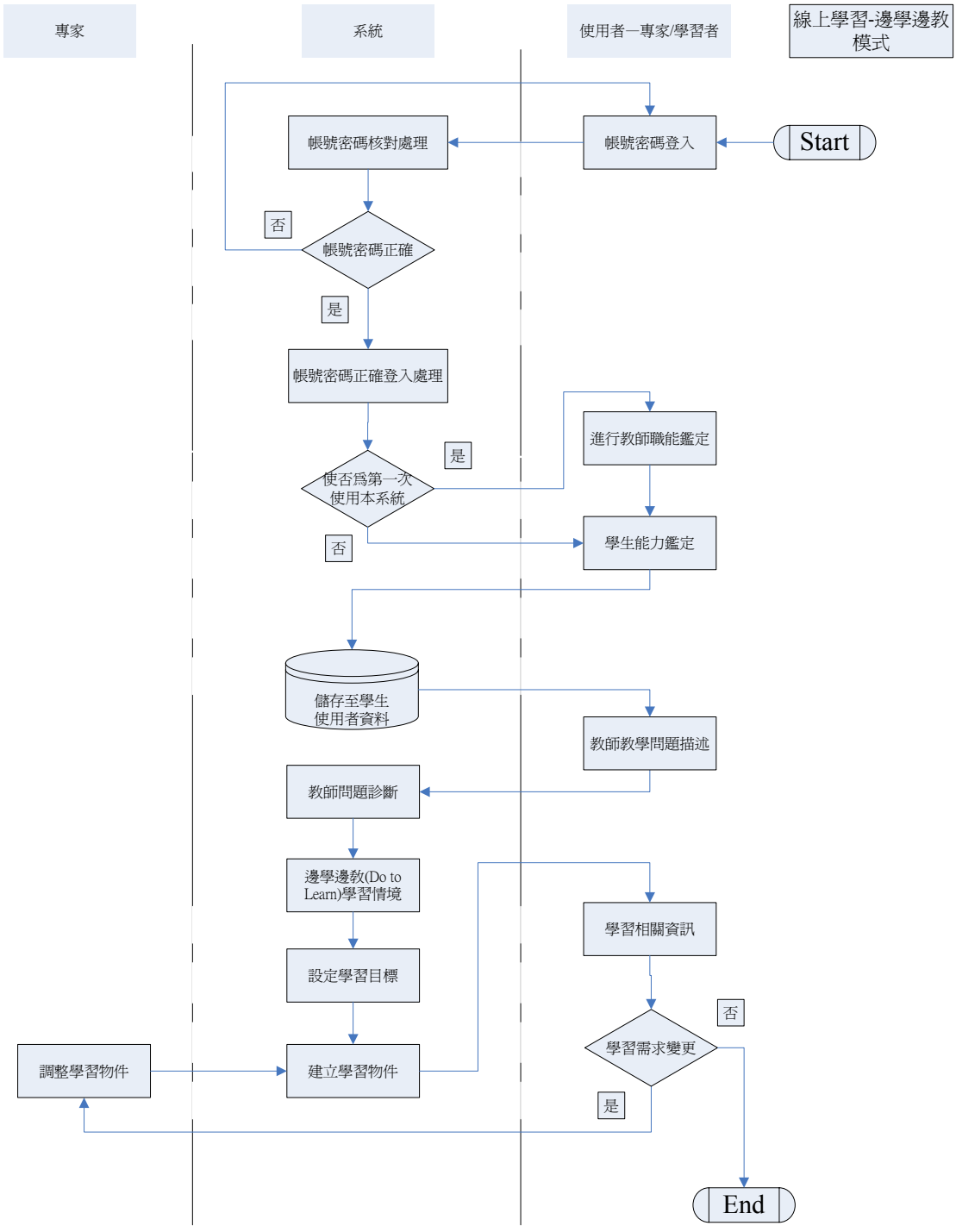
上學習之前系統會先進行教師職能的鑑定，鑑定出教師的教學職能後再進行學生能力的鑑定，鑑定學生的障礙程度與學習興趣，經由這些基本的能力鑑定過後系統會要求使用者將教學上的問題描述於系統上，之後系統會請使用者挑選合適自己的學習模式後再進行線上學習。

- 先學後教模式主要在針對這些問題設定學習目標，在針對學習目標建立學習物件及程序再讓使用者進行線上的學習。

- 邊學邊教模式主要差別在使用者可以針對學習的實際情況進行提出學習需求的變更，經由專家的確認後再進行學習物件的調整，調配出最符合使用者問題需求的學習模式。



圖十四 線上學習(先學後教模式)流程圖

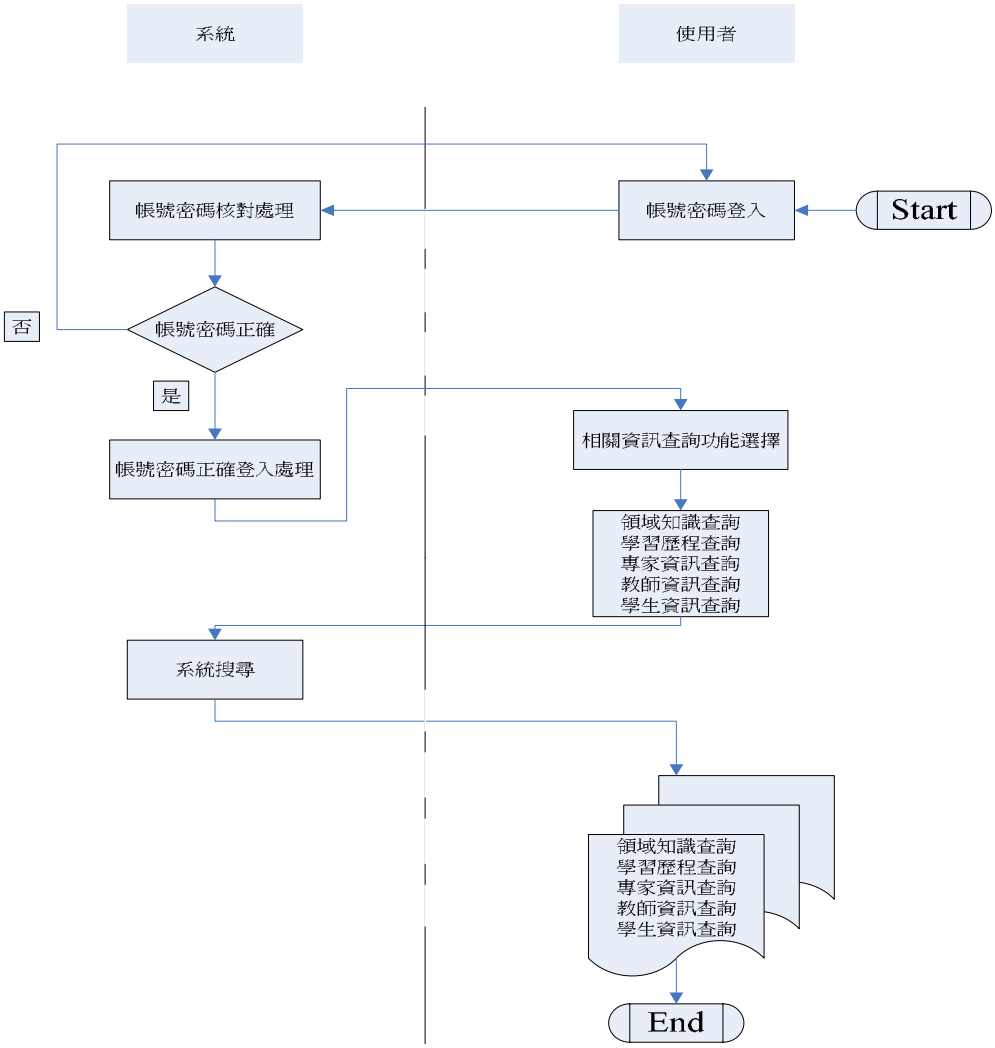


圖十五 線上學習(邊學邊教模式) 流程圖

2.5 相關資訊查詢

相關資訊的查詢，系統主要提供使用者可以進行領域知識、學習歷程、

專家資訊等等的查詢，讓使用者可獲得相關所需的資訊內容。



圖十六 相關資訊查詢流程圖

附件(三) 自動摘要數位學習平台討論區內容機制設計

摘要

隨著網際網路與多媒體等資訊科技的進步，數位學習漸漸成為學習的另一種重要形式，數位學習不受時間與空間的限制，建構出師生共同學習的環境。由於數位學習平台本身使用環境上的限制，使得老師與學生、學生與學生間的互動有所限制，目前絕大多數是以數位學習平台上的討論區為媒介。討論區充滿大量互動的資訊供師生學習與分享，由於資訊過量，使得師生需花費大量的時間尋找所需的資訊。而研究中指出，這些資訊隱藏著許多有用的知識，目前是透過人工的方式將資訊整理成知識，費時費力。爲了降低人工方式整理的人力與搜尋的時間，本研究希望藉由現有的中文斷詞與文件自動摘要的技術，設計一自動摘要數位學習平台討論區內容機制，來輔助討論區管理者將討論區中的內容自動彙整成常見問答集(Frequently Asked Questions)，有效率的將討論區中的知識分享給所有的師生使用。

一、緒論

隨著網際網路與多媒體等資訊科技的進步，越來越多人利用數位學習來進行教學活動，因此數位學習漸漸成為學習的另一種重要形式。數位學習主要是不受時間與空間的限制，建構出師生共同學習的環境。Moore(1996)認為數位學習應包含”交談”與”結構”兩大要素，其中”交談”指在教育活動中，學習者、教師以及活動三者之間可以相互溝通。但由於數位學習模式不像傳統的教學模式，可以容易讓老師與學生實際面對面的接觸，所以老師與學生的交流有一定的限制。LERN(1998)曾提出數位學習平台主要有 7 種服務，其中提到，若要方便課程討論與師生互動的服務，必須組織網路論壇(Forum)區；另外也提到，可運用電子佈告欄(BBS)、討論區等服務針對特定議題分享不同觀點。因此討論區

成為數位學習平台上有效讓老師與學生、學生與學生間的重要互動服務。當學生發生問題時，學生可以在平台上詢問，或是互相討論課業，老師也可以透過學習平台發佈學習進度，或是為學生解答疑惑。

目前討論區之互動透過文字進行，可以完全記錄互動過程，在日積月累的情況下，形成龐大的資訊供學習者學習。但由於討論區經常經常出現一些無意義的聊天文章，過量或品質參差不齊的資訊，並未帶來相對的好處，反而造成學習者學習的障礙，學習者需花費更多的時間來過濾無用的資訊。

從知識管理角度觀察，長期以來的常見問答集(Frequently Asked Questions, FAQ)已經是討論區既有之知識分享格式，往往是由其管理者負責彙整討論內容重點，並以問答方式摘錄，提供學習者一個的便利方式進行該討論主題之系統化資訊搜尋功能。由於過量的資訊亦造成了資訊管理者的負擔，要整理如此龐大的資料，需要花費非常多的人力與時間，隨著討論區的普及，已氾濫到很高比例的管理者疏於管理或甚至於不去管理，反而造成 FAQ 知識形式的相形式微。在知識管理意識的抬頭的大環境中，大家都體會到知識分享的好處與價值，這樣一個既有的 FAQ 工具與分享現況，更需要關注與保存。而周鉦琪(2003)提到在在討論區上所累積的文章中，隱藏許多有用的知識，可透過資訊技術來協助整理及找出這些有用的知識。

討論區的文章與 FAQ 屬文件摘要的轉換工作，現今的文件自動摘要技術相關研究已有相當的應用水準。因此，如何整合現有資訊技術及網路技術來輔助人工方式產生 FAQ，以降低人力與時間的需求，是本研究欲解決的問題。

因此本研究設計一自動摘要數位學習平台討論區內容機制，來輔助討論區管理者將討論區中的文章有效率地整理與集結，使得這些有用的知識能分享給更多的人使用。

二.文獻探討

2.1 文件自動摘要

文件自動摘要之研究起源於 1950 年代。Luhn（1958）乃建立一套文件摘要系統，當時提出此系統之目標乃希望能協助讀者較快速、簡潔地閱讀論文資料，並且方便使用者找尋有效之資訊。

依摘要產生方式不同，自動摘要技術主要可分為兩種方法。第一種方法稱為「摘錄（Abstract）」，意指針對文件內容進行理解，擷取文件關鍵意涵，將文件內容分析後重新編寫，以產生一份與原有文章句子不完全相同之摘要。第二種方法稱為「擷取（Extract）」，即將原有文章句子擷取一定比例作為摘要。由於重新編寫一份摘要困難，所以目前文件自動摘要以「擷取」方式為主要作法，故如何挑選重要句子則為此方法必須考慮之要素。

依摘要所期望達到目的之不同，自動摘要技術可分為三種類型。第一種為指示性摘要（Indicative Summary），即是提供閱讀者足夠資訊，使其可根據這些資訊判斷並決定是否閱讀原始文件。第二種為資訊性摘要（Informative Summary），其乃提供豐富的資訊內容，有時甚至可取代原始文件。第三種為評論性摘要（Evaluative Summary），其目的即是以摘要形式對原始文件進行評論，可提供閱讀者不同角度的論斷。

依原始文件數量不同，自動摘要分成兩大類型。第一類型即是「單一文件摘要（Singular Document Summarization）」，其乃將單篇文件的內容精簡化與重點化，並注重於能否有效地刪減不必要之資訊，以能留下真正代表文件內涵之資料。另一類型則為「多文件摘要（Multiple Document Summarization）」，其乃將多篇探討類似主題或事件之文件融合一起。該方法除了刪減無用之資料外，尚需有效率地過濾重複於多篇文章中出現之資訊。

文章摘要內容篩選原則上以句子為單位，往上提昇至內文段落(Salton et al. ,1997; 黃純敏，2001)，進而至多文段落或句子，因此單文摘要與多文摘要類似(翁鴻加，2001)，只不過多文摘要在方法運用上因範圍較廣而有較多的步驟處理程序(黃思萱，2002；沈建誠，2001)。

目前商業用途的摘要往往摘錄文章最前面的句子作為摘要，例如 Lycos 搜尋引擎則提供前幾百字元作為該文章之摘要(Neff and Cooper,1999)，Mead Data Central 的 Searchable Lead 資料庫也提供前 60 字、150 字及 250 字為該文章之摘要(Brandow et al. ,1995)。從文獻研究發現，最佳文章摘要比例約為 20% (Morris et al. , 1992)，Neff and Cooper (1999)提及自己實驗及 Verity 軟體開發者都指出至少要四句話才讓使用者能夠主觀地接受這樣的摘要。Goldstain et al.(1999) 的研究也建議一篇文章的摘要至少要三至五句話。

績效上來看，較複雜的方法未必有顯著的差異，例如 Namoto and Matsumoto(2001)以最小描述原則(Minimum Description Length Principle, MDL)延伸 C4.5 決策數演算法與一些非學習基礎(Unsupervised)的演算法比較，發現一種 K-means 分群演算法的績效不亞於技術層次應用較複雜的方法學習督導。Zhi et al. (2001) 開發一個以代理人為基礎的自動文字摘要系統 iTSum，但受限於目前 NLP 的發展，仍然無法與人工摘要的結果相提並論。Brandow et al. (1995) 指出要自動產生可讀性高的摘要的目標，以當時的技術而言，最多僅能實作出示範系統或非常受限的應用領域系統。葉鎮源(2002)使用文件集為基礎(Corpus-based approach)及潛在語意分析(Latent semantic approach)兩種技術，於壓縮比 30%下，召回率分別為 52%及 45.6%，效益均不差。Knight and Marcu (2002)研究語料基礎的噪音頻道(noisy-channel)及決策數兩種方法。並認為語料基礎的方法能提供較好的摘要結果。Gong and Liu(2001)以傳統的資訊檢索(Information

Retrevial, IR)及潛藏語意(latent semantic)分析技巧兩種方法進行，這兩種方法評估的結果是無顯著差異，因此建議採用簡單傳統的 IR 方法而捨較複雜的。

在技術限制下，基本方法應用之外，一些研究也強調系統整體實用性。如 Lehmam (1999) 針對科學及技術文件開發一個法文的自動摘要系統 RAFI 時，及強調其簡易使用、友善介面及快速、並能滿足使用者需求。Neff and Cooper (1999) 開發一個提供摘要的查詢系統 ASHRAM(Active Summarization and Markup)，雖然後端使用以語料為基礎(Corpus-based)的自然語言處理技術(Natural Language Processing, NLP)，但強調提供一個主動輔助使用者瀏覽文件的前端介面設計。所以，其介面搜尋的結果除了有原始全文外，並提供關鍵字、摘要及連結到本文的超連結。Rothkegel (1995)提出一個三層式文字模式，分內容、功能到格式剖析文章，該模式較適用於結構性較強的領域，例如該文中引用科學領域的文件來說明內容、功能與格式的規則。

2.2 中文斷詞

自動化文件摘要的首要步驟就是斷詞，然而中文文件斷詞處理有別於英文文件的斷詞程序。英文詞彙的界線很容易區別，文件中的詞(word)與詞間以空白隔開，僅需以空白為中斷點，即可斷出獨立的詞彙。而中文句子因為字字相連，詞與詞間並無明顯的界線，因而不易確認詞彙的界線(張智星，2000)。Chen,Ma 曾提到中文字義廣博精深，雖然字相同，但是只要位置不同，往往就產生不同的字義，所以在進行中文內容解析時，會產生許多的困擾。

目前中文文件斷詞主要分為統計式斷詞(Fan and Tsai, 1988; Sproat and Shih, 1990)、詞庫式斷詞(Chen and Kiu, 1992)及混合式斷詞(Nie, Briscbois and Ren, 1996)三種。

統計式斷詞，需藉由大量的文件或語料庫(corpus)的統計資料(詞頻、門檻值)，以鄰近字元出現的頻率高低來決定斷詞的位置。統計式斷詞適合大量資料的處理，主要依據機率統計值來決定斷詞的位置，優點是不需專家定義詞彙，執行效率高，能有效解決詞庫在擷取複合名詞、專有名詞及新生詞彙的問題。但統計式斷詞大多只能處理二字詞以內的詞彙，如果詞長大於二時，則斷詞的效率會大幅降低，及提高演算法的複雜度(Nie, Briscbois and Ren, 1996)。由於語料庫與應用領域有關，不同語料庫間的統計資料不適合互用，極易影響斷詞的正確性。

詞庫式斷詞，是目前最為普遍使用的斷詞方式，主要是利用現有詞庫與文件進行比對，一般最常使用的方式為長詞優先法。然而詞庫式斷詞的缺點受到詞庫品質的影響很大，對於複合詞彙、大多數的專有名詞與新生詞彙無法辨識。為了要提高斷詞的正確性，必須不斷的更新詞庫的內容。另外，有學者將詞庫式斷詞法，輔以構詞規則，發展出規則式斷詞法(陳克健等，1986)，以提昇斷詞品質。

混合式斷詞，將詞庫式斷詞法與統計式斷詞法整合(Nie, Briscbois and Ren, 1996)。利用詞庫式斷詞找出不同的斷詞組合，再利用詞彙的統計資料，找出最佳的斷詞組合。另外，陳稼興、謝佳倫與許芳誠(2000)提出以遺傳演算法(Genetic Algorithms)為基礎的中文斷詞模型，用以處理中文斷詞的問題。其類似統計式斷詞的做法，透過文章的訓練自行產生詞庫，其優點可避免人為介入的不客觀性，也可避免浪費人力資源。

本研究使用中研院 CKIP 中文斷詞系統是屬於混合式的方式斷詞，使用者可以經由建立 Winsock 與中研院斷詞系統做連線，使用 XML 的格式來傳送和交換欲斷詞的文章，產生斷詞結果與斷詞標記，再加以去除冗詞後產生關鍵詞。

2.3 句子相似度計算

文件摘要的目的是在於將重要的句子摘錄成一篇簡短的文章，輔助使用者能夠在較短的時間內了解文章的內容，為了要將重要的句子結合成摘要，需要評估句子的重要性。一般研究還是以較為客觀的關鍵詞法作為評估句子的重要性的準則(邱立豐，2002)。

一般評估文章的重要性可考慮詞彙在文章中所出現的頻率及關鍵詞彙所在的位置，主要以 TF*IDF(Term Frequency /Inverse Document Frequency)及相似度兩種權重計算方式 。 TF*IDF 的計算方法，其字詞的權重與詞頻成正比，而其出現的文章篇數成反比，依此方法計算出的字詞的權重值作為評估句子重要性的依據。 句子的相似度計算，則是利用句子間關鍵詞重疊多寡來求句之間的相似度大小，一般會設定一個門檻值作為判斷句子之間是否達到高相似度值，而在文章中與較多句子具有高相似度時，相對地代表此句子在文章中愈重要。

相似度的大小是藉由兩句子皆存在之關鍵字所佔的比重大小而決定，在計算相似度的方法主要有四種如表一所示：內績(Inner Product)、骰子(Dice)係數、Jaccard 係數及 Cosine 係數(Brandow et al., 1995; Singhal et al., 1996)。表中 X 與 Y 則分別代表關鍵字詞在文章之中出現的次數；X∩Y 表示在文章中共同出現之關鍵字詞的次數；X∪Y 表示在文章中所有關鍵字詞出現的總次數。

Similarity Measure sim(X, Y)	Evaluation for Binary Term Vectors	Evaluation for Weighted Term Vectors
Inner product	$\lvert X \cap Y \rvert$	$\sum_{i=1}^{t} x_i \bullet y_i$
Dice coefficient	$2\frac{\lvert X \cap Y \rvert}{\lvert X \rvert + \lvert Y \rvert}$	$\frac{2\sum_{i=1}^{t} x_i y_i}{\sum_{i=1}^{t} x_i^2 + \sum_{i=1}^{t} y_i^2}$
Cosine coefficient	$\frac{\lvert X \cap Y \rvert}{\lvert X \rvert^{1/2} \bullet \lvert Y \rvert^{1/2}}$	$\frac{\sum_{i=1}^{t} x_i y_i}{\sqrt{\sum_{i=1}^{t} x_i^2 \bullet \sum_{i=1}^{t} y_i^2}}$
Jaccard coefficient	$\frac{\lvert X \cap Y \rvert}{\lvert X \rvert + \lvert Y \rvert - \lvert X \cap Y \rvert}$	$\frac{\sum_{i=1}^{t} x_i y_i}{\sum_{i=1}^{t} x_i^2 + \sum_{i=1}^{t} y_i^2 - \sum_{i=1}^{t} x_i y_i}$

表一：相似度計算公式

Salton et al. (1997)將 Text Relationship Map 的概念應用在文件摘要的研究上，其從文件連結觀點探討百科全書內文段落之關聯性，並提出以段落(Paragraph)為摘錄單位的文件摘要系統，希望藉由相關段落的組合以克服文句連貫性的困難。Salton 在相似度的組成摘要上，提出了三種內文連結模式：

Global Bushy Path

在文章內與它句子鏈結最多的那一個段落被認為重要性最高。因此，會首先被挑選出來成為摘要的第一句，當第一個段落決定後，在從全篇文章中鏈結點次多的某一段，成為摘要的第二個段落。所以 Global Bushy Path 主要是以鏈結點的多寡為挑選準則，擷取排序在前的數段用以組合成摘要。由於鏈結點較多的段落，理論上所敘述的內容應該較為重要，因此此種做法所形成的摘要主題涵蓋範圍十分廣泛，然而上下段落的突兀可能造成閱讀的不順。

Depth-First Path

首先挑選分數最高或鏈結最多的當第一句，在此部分與 Global Bushy Path 相似，其差異點是如何挑選第二句以後的段落，其挑選的準則是選取在文章順序中與前一句最接近且相似度最高的一句，因此避免類似 Global Bushy Path 的問題，使得摘要的一致性與閱讀性提高。其最大的問題是在於摘要內容的一致性提高，並不見的能夠涵蓋原文所有的主題與概念，其涵蓋的主題範圍可能會侷限於與首段主題相關的敘述，而無法反映整篇文章的範圍，導致摘要內容的不完整。

Segmented Bushy Path

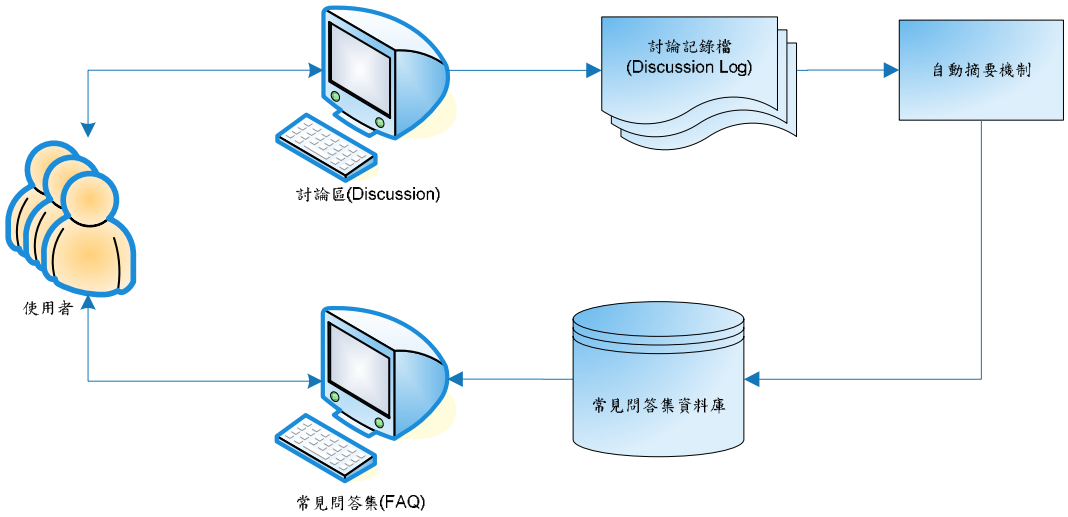
為了綜合以上兩種方鏈結方式的優點，在 Global Bushy Path 中加入 Text Segment 的概念，將一篇文章相鄰的組成分子，切割成多個 Segment，以 Global Bushy Path 的方式選取在各個 Segment 中最多連結點的段落，如此一來應該可增廣摘要的主題範圍。

黃純敏(2001)將三種內文連結模式，經評估實驗結果，發現其中 Global Bushy Path 在鏈結的一致性及內容廣度都比另外兩個方法有較好的成效。於是採用 Global Bushy Path 的方法，並以句子為擷取的比較對象，依據關鍵詞彙共同出現的頻率，引用 Jaccard coefficient 計算句子間的相似度值。全篇文章的分句權值，則為該句與其他句的相似度總和，亦即連結點越多的句子權值愈高，代表該句越重要。

三.研究架構

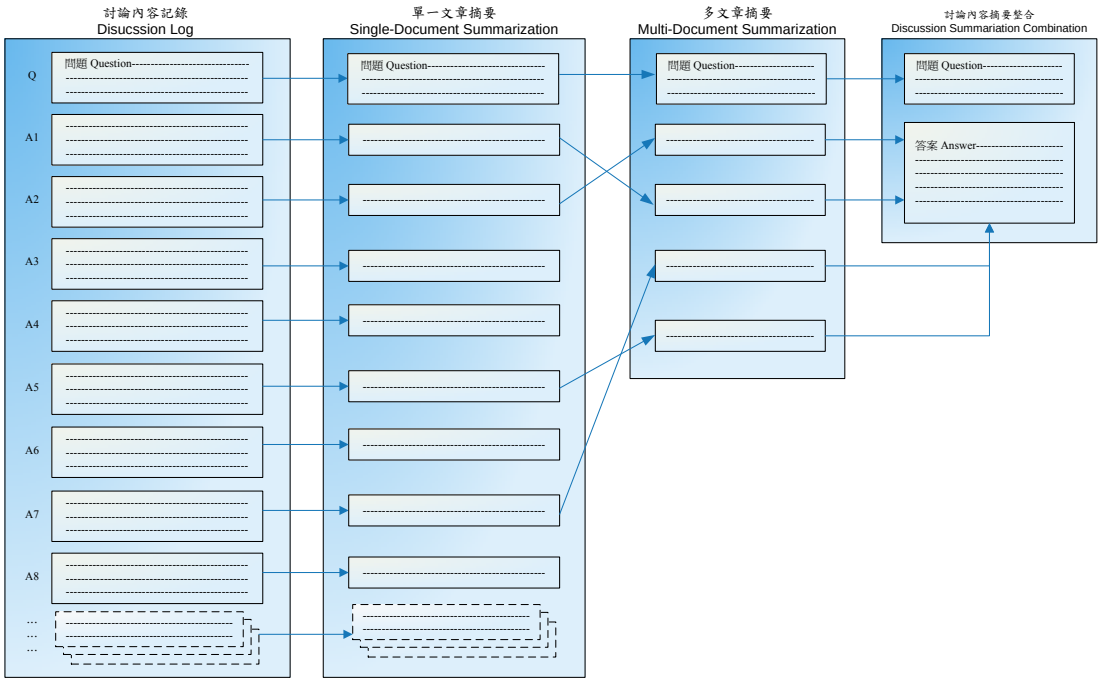
自動摘要的相關研究在國內外已行之有年，而討論區內容自動摘要的研究則屬一較新的範疇。本研究從字詞本身權重推估句子重要性的觀點出發採 Global Bushy Path 方法來計算句子權重，並擷取權重值排行在前的句子用以組合成摘要。

圖一為討論區內容與常見問答集使用情境圖，使用者可以使用討論區進行討論與瀏覽事項，或可以透過常見問答集進行常見問答題的搜尋與瀏覽，系統則會自動將討論記錄透過自動摘要機制將討論內容整理成常見問答集以儲存到常見問答集資料庫，作為常見問答集之資料來源。



圖一：討論區內容與常見問答集使用情境圖

由圖一情境圖得知自動摘要機制扮演著重要的角色，讓討論內容不需透過人工的處理自動的轉存到儲存區內。本研究將自動摘要機制進一步的分析，得到自動摘要的步驟，如圖二所示，主要分為三個步驟，單一文章摘要→多文章摘要→討論內容摘要整合。一般討論內容記錄為一個問題及回應此問題之答案，由於回應問題有些屬無意義的文章，因此需將與問題較相關之句子從單一文章中取出，因此各文章都取出較重要之句子，接著再將各文章中取出與問題較相關之句子，最後將問題與所取出之重要句子整合，形成討論內容摘要。

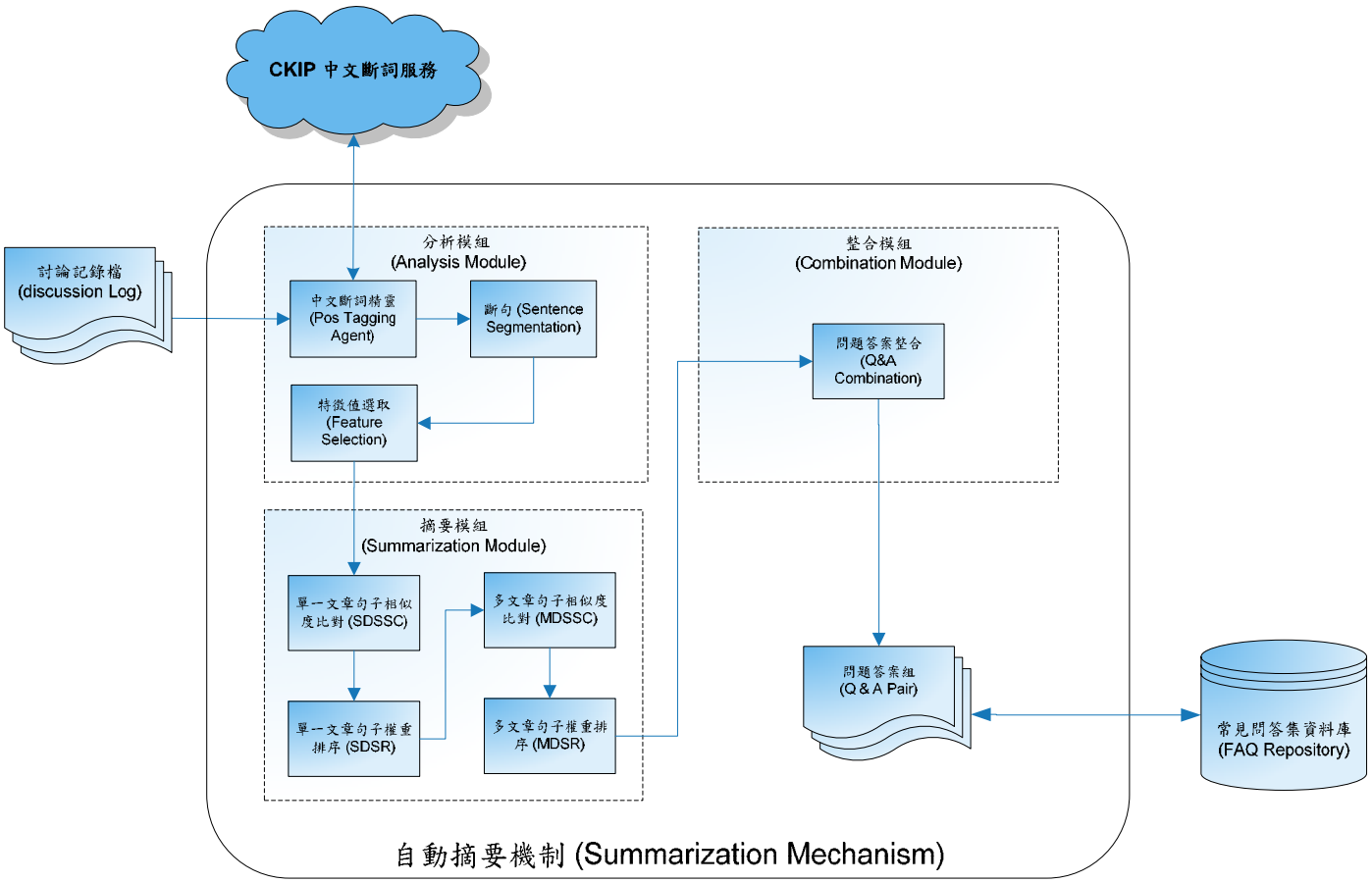


圖二：自動摘要的步驟圖

依據自動摘要的步驟，本研究設計自動摘要機制，主要將機制模組化，分為三個模組(如下圖所示)，第一個模組為分析模組，主要是將討論內容進行斷詞、斷句及句子選取特徵值。而第二個模組為摘要模組，透過二階段的相似計算找出重要之句子。第三模組為整合模組，將被篩選的重要句子與問題合併並存入資料庫中。

3.1 分析模組 (Analysis Module)

分析模組主要將各回應之文章送由 CKIP 斷詞服務進行斷詞，再依據斷詞之結果進行斷句及句子特徵值篩選。本研究針對模組中之元件做詳細之說明。



圖三：自動摘要機制之流程圖

3.1.1 中文斷詞精靈(POS Tagging)

中文斷詞精靈主要的功用於將輸入的討論內容記錄檔進行斷詞，本研究利用中央研究院詞庫小組(CKIP)的中文自動斷詞系統「Auto Tag」將這些將討論內容作斷詞及詞性標註的動作，目前 CKIP 開放線上斷詞服務，中文斷詞精靈以 API 呼叫 CKIP 斷詞服務，以 XML 為資料交換方式並利用 TCP Socket 連線傳送驗證資訊及文本至該伺服器，CKIP 斷詞服務經過處理後經由原連線傳回結果。圖四為 CKIP 斷詞服務回傳之範例。

圖四：CKIP 斷詞服務回傳之範例

3.1.2 斷句(Sentence Segmentation)

本研究之討論內容自動摘要是以句子為主要對象，所以在自動摘要的形成上，首先要對文章進行斷句。在文章斷句的處理，依據以下的原則

1. 文章中每一個句子與句子間皆有標點符號區隔。若無標點符號區隔，無法有效的區分出文章中的各個句子，如此便無法計算各獨立句子的相似度得分。
2. 斷句方面，以句號(。)、驚嘆號(！) 及問號(？)作為分隔符號。所有的標點符號，需同時考慮到半形與全形兩種情況。
3. 分隔文章句子時，需同時紀錄句子出現在文章中的位置(第幾篇的第幾句)。

在斷句的過程中，對於其他的標點符號並不做進一步的處理，而保持其原有

的面貌。

3.1.3 特徵值選取(Feature Selection)

在句子中，動詞與名詞通常是句子裡的關鍵核心，在自動摘要的文獻探討中，亦採用動詞與名詞當作重要詞的依據(黃純敏、吳郁瑩，1999)，因此本研究僅將動詞與名詞視為與文章內容最相關的重要詞彙。經由 CKIP 詞性標註，可得到該斷詞之詞性，並依下詞性表選取名詞及動詞為特徵值。表二為 CKIP 所定義的動詞與名詞詞性。

表二：動詞與名詞詞性表

POS Tag	Meaning
Na	普通名詞(Common noun)
Nc	地方名詞(Place noun)
Ncd	位置詞 (Location noun)
VA	動作不及物動詞(Intransitive verb)
VAC	動作類及物動詞(transitive verb class)
VB	動作類及物動詞(Single verb class)
VC	動作及物動詞(Single verb)
VCL	動作接地方賓語動詞(Active location object verb)
VD	雙賓動詞(Two words verb)
VE	動作句賓動詞(Verb sentence)
VF	動作謂賓動詞(Name verb)
VH	狀態不及物動詞(Status Intransitive verb)
VHC	狀態類及物動詞(Status transitive verb class)
VJ	狀態及物動詞(Status single verb)

3.2 摘要模組 (Summarization Module)

本研究為多文件摘要性質，將相似度計算分為兩階段進行，經由斷詞處理後，進行兩階段相似度計算，第一階段的相似度是計算單篇文件中，各個句子的相似度值，第二階段是計算多篇文件中，各個句子的相似度值；在第一階段計算完各句子單篇文章的相似度值，排序各篇句子的相似度值高低，再進行第二階段的處理，再取得第一階段各篇文章相似度值較高的前幾句來進行多篇文章句子相似度的計算，最後排序多篇文章之句子相似度值，取其相似度值較高的幾句，並依其先後位置順序形成討論區摘要。本研究以 Jaccard coefficient 作為句子相似度值的計算方法，Jaccard coefficient 對於重要句子的認定，以各個句子與其他句子連結的多寡而定。所謂句子間的連結關係，是指彼此間有出現相同關鍵詞彙，在短短字句中出現相同的關鍵詞彙，表示所討論的主題應該是近似的。理論上連結點較多的句子，表示該句與其他句子有較多重疊的關鍵詞彙，所敘述的主題應該較為重要；其公式如下：

$$\text{Jaccard coefficient} \quad \frac{|X \cap Y|}{|X|+|Y|-|X \cap Y|}$$

膟

膟　X 表 A 句中關鍵詞數目，

膟　Y 表 B 句中關鍵詞數目，

膟　$X \cap Y$ 表 A、B 句中重複的關鍵詞數目。

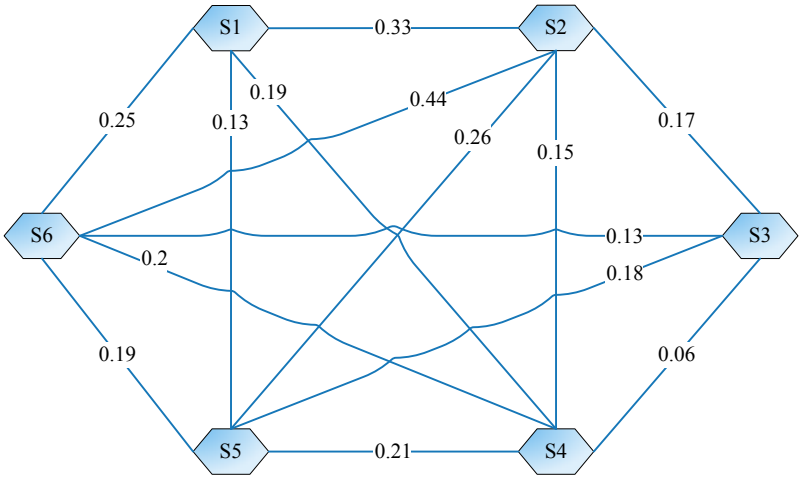
膟依照 Jaccard coefficient 在求得各句之間的相似度值後，相似度值會介於 0 至 1 之間，全篇文章的分句權值，則為該句與其他句的相似度總和，亦即連結點越多的句子權值越高，代表此句子越重要。

以下舉個範例說明之：

編	原句	特徵值	相似度	權重

號				
S1	有些特殊學生需要更多的特殊需求的學習環境，不管是普通班、資源班、集中式特教班、特殊教育學校，都應有其功能。	特殊 學生 需要 需求 學習 環境 普通班 資源班 特教班 教育 學校 功能 (11)	S1&S2 =5/(11+9-5)=0.33 S1&S3=0 S1&S4=4/(11+14-4)=0.19 S1&S5=3/(11+15-3)=0.13 S1&S6=3/(11+4-3)=0.25	0.90
S2	目前所提倡的融合教育，大部分都會偏向到學校環境的融合、與普通學生的融合、上多少普通班的課程等。	融合 教育 偏向 學校環境 普通 學生 普通班 課程 (9)	S2&S1 =5/(9+11-5)=0.33 S2&S3=2/(9+5-2)=0.17 S2&S4=3/(9+14-3)=0.15 S2&S5=5/(9+15-5)=0.26 S2&S6=4/(9+4-4)=0.44	1.36
S3	有時候在課程規劃方面，還有一種融合也是極其重要的～就是社區融合。	課程 規劃 融合 重要 社區 (5)	S3&S1=0 S3&S2=2/(5+9-2)=0.17 S3&S4=1/(5+14-1)=0.06 S3&S5=3/(5+15-3)=0.18 S3&S6=1/(5+4-1)=0.13	0.52
S4	融合教育的含意是及其廣泛，主要針對特殊需求學生如何與現實生活作相關連結，以改善其障礙狀況。	融合 教育 含意 廣泛 特殊 需求 學生 現實 生活 相關 連結 改善 障礙 狀況 (14)	S4&S1=4/(14+11-4)=0.19 S4&S2=3/(14+9-3)=0.15 S4&S3=1/(14+5-1)=0.06 S4&S5=5/(14+15-5)=0.21 S4&S6=3/(14+4-3)=0.2	0.80
S5	雖然特殊教育學校是比較集中式的狀況，但是如果在課程方面依據改善學生障礙的模式，安排社	特殊 教育 學校 狀況 課程 改善 學生 障礙 模式 安排 社區 鄰近 交流 實施 融合 (15)	S5&S1=3/(15+11-3)=0.13 S5&S2=5/(15+9-5)=0.26 S5&S3=3/(15+5-3)=0.18 S5&S4=5/(15+14-5)=0.21 S5&S6=3/(15+4-3)=0.19	0.97

	區或是鄰近學校交流其實都可以實施融合教育。			
S6	不一定只是要和普通班的學生在一起，才教育融合。	普通班 學生 教育 融合 (4)	S6&S1=3/(4+11-3)=0.25 S6&S2=4/(4+9-4)=0.44 S6&S3=1/(4+5-1)=0.13 S6&S4=3/(4+14-3)=0.2 S6&S5=3/(4+15-3)=0.19	1.21



圖五：Global Bushy Path

3.3 整合模組 (Combination Module)

摘要模組將多篇文章的重要句子篩選後，接著整合模組需將問題與摘要內容進行整合並存入 FAQ 資料庫中。為提昇使用性及降低摘要不完整下之不滿意程度，摘要的表達，將以重要句子條列之，並可連結閱讀原文，並且將關鍵字條列於摘要之前，讓使用者可有充分瀏覽關鍵字、摘要及全文之自由度及彈性。

四.結論

本研究利用 CKIP 的中文斷詞服務及 GBP 方法設計一個自動摘要數位學習平台討論區內容機制，將討論區內容彙整並摘錄重點產生成 FAQ，以輔助網站管理者或討論區版主輕鬆地及有效率地進行知識擷取與轉換的工作環境，並快速

的將討論區中的知識分享給所有的師生使用。

在討論區上一般會參雜英文詞彙，而部分英文詞彙也隱含有用的訊息，而本研究所採用之 CKIP 斷詞服務無判斷其詞性，未來的研究方向可對於夾雜之英文詞彙需進行特別處理，以增加摘要擷取廣度與效果。

六.參考文獻

1. 中研院詞庫小組，「中文斷詞系統」，來源：http://ckipsvr.iis.sinica.edu.tw/。
2. 周鉦琪，謝盛文，陳年興。利用網際網路上顧客討論社群發掘產品生命週期。電子商務與數位生活研討會，pp.97。2003。
3. 邱立豐，互動式概念查詢應用於網路文件自動摘要之效益，*資訊管理研究所碩士論文*，國立雲林科技大學，2002。
4. 張智星，中文新聞摘要，*資訊工程研究所碩士論文*，清華大學，2000。
5. 陳克健、陳正佳、林隆基，中文語句的研究—斷詞與構詞，*中央研究院資訊所技術報告*，TR-86-006，1986。黃思萱，以關鍵詞分群為基礎的多文件摘要，*資訊管理研究所碩士論文*，國立台灣科技大學，2002。
7. 黃純敏，多語文（中英文）超文件自動摘要與評估，*行政院國家科學委員會專題研究計畫成果報告*。計劃編號：NSC89-2416-H-224-053，2001。
8. 黃純敏、吳郁瑩，網路文件自動摘要，*台灣區網際網路研討會 TANET'99*, 國立中山大學承辦，1999。
9. 葉鎮源，文件自動化摘要方法之研究及其在中文文件的應用，*資訊科學研究所碩士論文*，國立交通大學，2000。
10. Brandow, R., Mitze, K. and Rau, L. F., "Automatic condensation of electronic publications by sentence selection", *Information Processing & Management*, Vol. 31, No. 5, pp. 675-685, 1995.
11. Brandow, R., Mitze, K. and Rau, L. F., "Automatic condensation of electronic publications by sentence selection", *Information Processing & Management*, Vol. 31, No. 5, pp. 675-685, 1995.
12. Brandow, R., Mitze, K. and Rau, L. F., "Automatic condensation of electronic publications by sentence selection", *Information Processing & Management*, Vol. 31, No. 5, pp. 675-685, 1995.
13. Chen, K. J. and Kiu, S. H., "Word identification for mandarin Chinese sentences", *Fifth International Conference on Computational Linguistics*, Nantes, France,

pp.101-107, 1992.

14. Fan, C. K. and Tsai, W. H., "Automatic word identification in Chinese sentences by the Relaxation Technique", *Computer Proceeding of Chinese and Oriental Languages,* Vol. 4, No. 1, pp. 33-56, November 1988.
15. Goldstain, J., Kantrowitz, M, Mittal, V. and Carbonell, J., "Summarizing text documents: sentence selection and evaluation metrics", in *Proc. Of ACM SIGIR'99*, Berkeley, CA, August 1999.
16. Gong, Y. and Liu, X., "Creating generic text summaries", *Sixth International Conference on Document Analysis and Recognition*, 9/10-9/13, Seattle, WA, USA, pp. 903-907, 2001.
17. K. J. Chen, W. Y. Ma, "Unknown Word Extraction for Chinese Documents,"Proceedings of COLING, pp. 169175, 2002.
18. Knight, K. and Marcu, D., "Summarization beyond sentence extraction: a probabilistic approach to sentence compression", *Artificial Intelligence*, Vol. 139, pp. 91-107, 2002.
19. Lehmam, A., "Text structuration leading to an automatic summary system: RAFI", *Information Processing and Management*, Vol. 35, pp. 181-191, 1999.
20. LERN（Learning Resources Network）, Online education：Growing presence and growing pains, Lifelong Learning Today, 6(1), pp 6-7 , 1998.
21. Luhn, H. P., 1958, "The automatic creation of literature abstracts," *IBM Journal of Research and Development*, pp. 159-165.
22. Moore, M. G. & Kearsley, G., Distance Education：A Systems View.Belmont：Wadsworth, 1996.
23. Morris, A.G., Kasper, G.M. and Adams, D.A., "The effects and limitations of automated text condensing on reading comprehension performance", Information Systems Research, March, pp. 17-35, 1992.
24. Neff, M. S. and Copper, J. W., "ASHRAM: active summarization and markup", in *Proceedings of the 32nd Hawaii International Conference on System Sciences*, Maui, HI, USA, 1999.
25. Nie, J., Briscbois, M. and Ren, X., "On Chinese Text Retrieval", *Conference*

Proceeding of ACM-SIGIR, Zurich, pp. 225-233, August 1996.

26. Nomoto, T. and Matsumoto, Y., “An experimental comparison of supervised and unsupervised approaches to text summarization”, *IEEE International Conference on Data Mining*, San Jose, CA, USA, 11/29-12/02, pp. 630-632, 2001.
27. Rothkegel, A., “Abstracting from the perspective of text production”, *Information Processing & Management*, Vol. 31, No. 5, pp. 777-784, 1995.
28. Salton, G., “Automatic Text Processing”, *Addison-Wesley Publishing Company*, New York, pp.328-338, 1989.
29. Salton, G., Singhal, A., Mitra, M. and Buckley, C. “Automatic text structuring and summarization.” *Information Processing & Management*, 33(2), pp. 193-207, 1997.
30. Singhal, A., Salton, G., Mitra, M. and Buckley, C. "Document length normalization," Information Processing & Management, Vol.32, pp.619-633, 1996.
31. Zhi, Z., Hin, H. K. P., Gay, R. K. L, Lin, G. W., and Yang, L. S., “iTSum: one agent-based system for automated text summarizing”, *International Conference on Information-Technology and Information –Network*, Vol. 3, Beijing, China, pp. 18-25, 2001.

附件(四) 問題與需求語意分析

摘要

隨著科技進步，人們習慣於網路上查詢，問題的描述往往是準確搜尋資料的關鍵，要如何解決使用者所描述的問題是本研究的主要目的。本研究提出一方法用以解析使用者所描述之問題涵義利用標記詞性，將關鍵字找出來，並利用統一模型語言(Unified Modeling Language，UML)之類別圖關係來建構出語意網概念模型，配合 ontology 技術加以延伸出更廣闊之概念，將建構的概念加入權重及過濾，以圖形化語意網表示，讓使用者更了解更多問題可延伸的資訊，進而解決使用者問題。

一、緒論

網路上充滿著豐富的資料，一般人上網找尋資料，往往因為描述問題的不清楚，而影響搜尋結果。如何準確的解析使用者所描述問題涵養是一個極大挑戰。在本研究中我們提出以圖形化語意轉換(Graphical Semantic Transformation Mechanism)及概念分解機制(Concept Decomposition Mechanism)為核心。其中圖形化語意轉換包含兩個主要子模組：使用者問題之語意分析模組(User Semantic Analysis Module)及圖形化語意網路轉換模組(Graphical Semantic Net Transformation Module)。透過這兩個子模組能將使用者描述的問題，利用自然語言處理與斷詞(Natural Language Processing and Segmented)技術轉成電腦可理解的網狀結構圖形，於知識庫中進行知識擷取比對，搜尋出使用者所需的資料。在知識庫中如搜尋不到使用者所需的資訊，我們會透過架構中之概念分解機制，將完整的概念進行分析拆解後提供給網頁搜尋引擎搜尋，來讓使用者獲得更多相關資訊的目的。

本研究主要工作項目：

（1）問題描述之語意解析及詞性標記。

（2）問題語意之關聯及延伸。

（3）將問題與 Domain Ontology 結合語意延伸。

（4）將問題轉換為圖形化語意網方式表示。

本研究預計完成工作項目：

（1）將問題描述之語意解析及詞性標記。

（2）問題語意之關聯及延伸。

本研究已完成工作項目：

（1）問題描述之語意解析及詞性標記。

（2）問題語意之關聯及延伸。

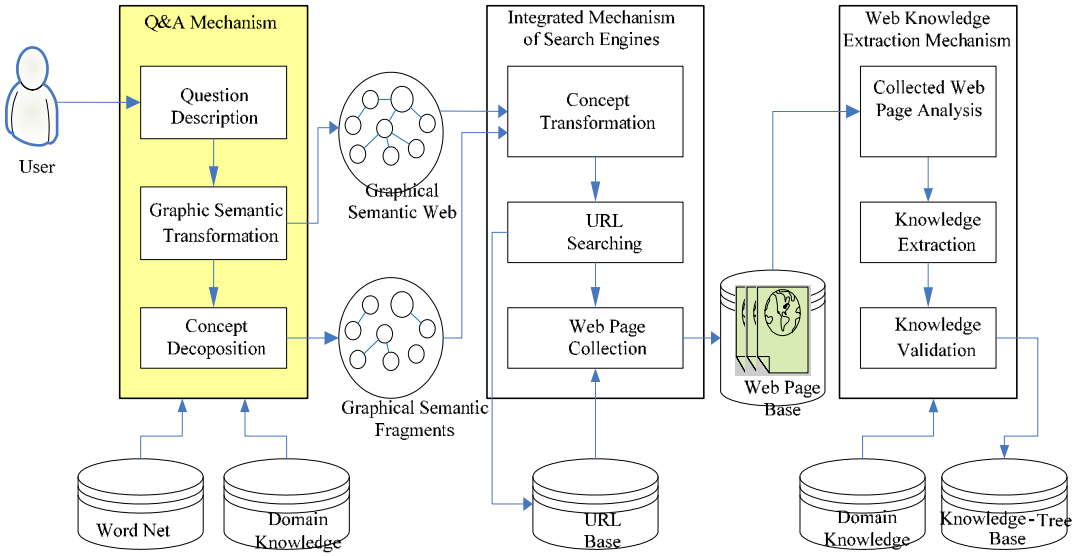
本研究未來工作項目：

（1）將問題與 Domain Ontology 結合語意延伸。

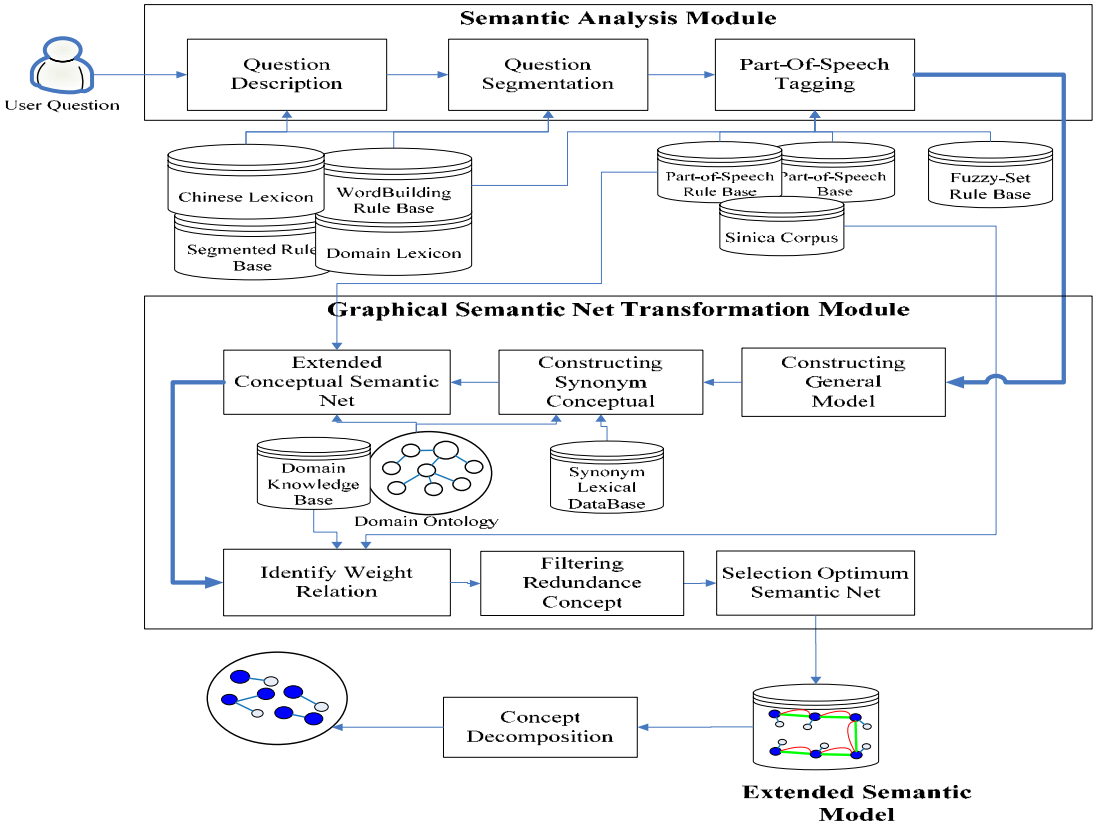
（2）將問題轉換為圖形化語意網方式表示。

二、研究架構

本研究主架構如圖一、圖二所示，可分為二個部分：語意分析機制(Semantic Analysis Module)及圖形化語意網轉換機制(Graphical Semantic Net Transformation Module)。



圖一 Graphical Semantic Net Transformation Mechanism



圖二 圖形化語意網轉換機制

圖形化語意轉換機制包含：語意分析模組(Semantic Analysis Module)；圖型化語意轉換模組(Graphical Semantic Net Transformation Module)幫助我們在這階段將問題描述產出圖形化語意網(Graphical Semantic Net)及概念分解機制。

（一）Semantic Analysis Module

利用數種資料庫來幫助問題做語意分析及語意轉換，包括問題之斷詞(Segmentation)、詞性標記(Part-Of-Speech Tagging)、語意延伸、過濾、建構概念模型及概念拆解，其步驟主要功能如下：

（1）Question Description Module

提供一個使用者介面讓使用者進行問題描述，將問題送給Question Segmentation Module。

（2）Question Segmentation Module

主要功能有問題斷詞(Question Segmentation)、字詞合併(Merging Word)、定義候選詞組(Candidate Phrase)、挑選詞組(Selection Phrase)及合併詞組(Merging Phrase)。分別說明如下：

1.Question Segmentation

依使用者描述之問題，利用中文詞庫(Chinese Lexicon)與斷詞規則的依字詞頻者最高者為優先(Sentence Segmentation)的規則，將問題拆解成單獨的字詞(Word)。

2.Merging Word

利用構詞規則庫(Word Building Rule Base)中定量複合詞(Determinative Measure Compounds)及四字疊詞(Reduplications)與中文詞庫做比對，把較小的字詞合併成較長的詞，稱為詞組(Phrase)。

3.Identifying Candidate Phrase

將合併的詞組，利用構詞規則與中文詞庫列出所有可能的詞組，成為候選詞組(Candidate Phrase)。

4.Selection Phrase

將定義後詞組，利用斷詞規則庫(Segmented Rule Base)之長詞優先、標準差小的優先、附著語素最少者優先、定量複合詞中字數最少者優先、一字詞詞頻最高者者優先、總詞頻最高者優先，以這六條規則做挑選。

5.Merging Phrase

被挑選之詞組，利用構詞規則，把彼此能結合成長詞的詞組做合併。

（3）詞性標記(Part-Of-Speech Tagging)

被合併完之詞組，先以平衡語料庫(Sinica Corpus)建立二階馬可夫語言模型[2]，再依詞性庫(Part-Of-Speech Base)及詞性規則庫(Part-Of-Speech Rule Base)並運用統計法計算詞類連結出現之機率。

（二）Semantic Net Transformation Mechanism

本機制功能為將語意分析模組標記後的詞組來建構一般化模型、延伸同義詞概念、擴展概念語意網、定義詞組權重、過濾無效概念及挑選最佳語意網，目的為將語意轉換成圖形化。其說明如下：

（1）建構一般化模型(Constructing General Model)

將標記後的每個關鍵字與Domain知識庫的詞性做比對，利用UML中的類別圖一般性關係、聚合關係、限定關聯、、相依性、可瀏覽性及類別多重性的所有

可能找出來，藉由這些關係建構出一般化模型。

（2）延伸同義詞概念(Extended SynonymConceptual)

建構後的關鍵字與同義詞庫做詞性及詞頻比對，將同義詞找出來，利用此關係更能了解語意的所有資訊。

（3）擴展概念語意網(Extended Conceptual Semantic Net)

被建構出的各個概念，利用 Domain Ontology 及知識庫(Knowledge Base)去延伸相關概念出來，形成語意網。

（4）定義權重關係(Identify Weight Relation)

產生之語意網，利用正規化概念分析理論，計算每個延伸及問題概念間之關係定義出來，形成延伸性語意網。

（5）過濾無效概念(Filtering Redundancy Concept)

被定義之概念，利用知識庫與概念做 TF-IDF 計算，設立一參數門檻值，把參數低於門檻者過濾掉。

（6）挑選最佳語意網(Selection of Optimum Semantic Net)

定義後之概念，給予權重做為排序挑選，把權重較高者挑選出來。

(三) Concept Decomposition Mechanism

被挑選後語意網，進行概念拆解，再與定義後的各概念做組合，而組合後概念與知識庫以 TF-IDF 方式做權重計算，權重高者做為關鍵字(Keyword)，權重低者則需再與其他概念做組合，直到各概念組合完成，讓下步驟整合型網頁搜尋引擎機制做搜尋處理。

三、結論

本研究提出一套依使用者問題為導向，利用數個規則庫與資料庫完成斷詞與標記，並以正規化概念去分析建構語意網，搭配本體論形成概念性的階層關係與延伸，由於延伸概念太多，所以透過概念與概念間之關係權重，設立一門檻值修正過濾無效的概念，產生圖形化語意網。

附件(五) 應用領域本體論設計整合網路搜尋引擎機制

近來由於知識經濟快速發展，以致於相關知識的蒐集、獲取、整合、儲存、管理、分享與運用之重要性相對提升，網路上充滿著豐富的知識，如何以自動化的方式有效利用網路上的資源提供使用者所需的知識是一項很大的挑戰。

本研究設計建構擁有過濾與排序機制的搜尋引擎(search engine)，並結合了網頁內容探勘(web content mining)、資訊檢索(information retrieval)與領域實體論(domain ontology)相關技術，主要是針對網路搜尋後的資訊進行資訊含量之計算，如摘要及標題；透過演算法刪除格式不完整、有重覆性與廣告等資料，並依資訊含量多寡給予權重，若資訊含量介於本研究所設立之可接受範圍，便利用領域實體所建立的法則計算詞彙之間的相似程度，再給予適當權重，並依權重高低逐一排序，最後將網頁內容存入儲存區，此結果可提供給使用者解決問題之參考，節省使用者自行過濾檢索時間並降低頻寬負載量。目前研究著重於國小數學學習障礙領域方面，希冀日後可廣泛應用於其他領域。

關鍵詞：搜尋引擎、網頁內容探勘、資訊檢索、實體論

一、緒論

隨著資訊科技日新月異，網路資源越來越豐沛且複雜，上網尋找資料變成解決問題的方法之一，網路上的資訊屬於超大型資料庫，目前各家搜尋引擎功能相當強大，導致所搜尋出的網路內容重複性太高或不符合使用者的需求等情況產生，因此目前使用的搜尋引擎一般而言有下列問題 [7]：

(1) 網路資訊成長迅速，單一搜尋引擎愈來愈難處理龐大的資訊空間。
(2) 多具引擎之搜尋結果所顯示的資訊量重複性太高，使用者需花費很多的時間與精神，嘗試在這些檢索結果中找出自己真正需要的資訊。
(3) 無意義的廣告伴隨著搜尋器而出現。

由此而知，網路上相關知識的蒐集、獲取、整合、儲存、管理、分享與運用之重要性相對提升。如何將使用者的問題或是需求轉化成一個圖形化的語意網路模型，使用此模型來描述使用者所提出問題的概念，並將模型中的關鍵字分別在網路的搜尋引擎中尋找相關網頁，透過本研究所設計的過濾排序機制進行比對工作找出真正貼切原意的摘要及網頁內容，最後經由網頁內容擷取與格式轉換以方便提供給使用者利用。

二、研究架構

為了有效搜尋與擷取網頁內容，本研究架構分為三個部分，如圖一所示：

(1) 前處理機制

・concept transformation

・keyword extraction

・specialized keyword composition

(2) 整合式搜尋機制：

・integration searching

(3) 後處理機制

・format standardizing

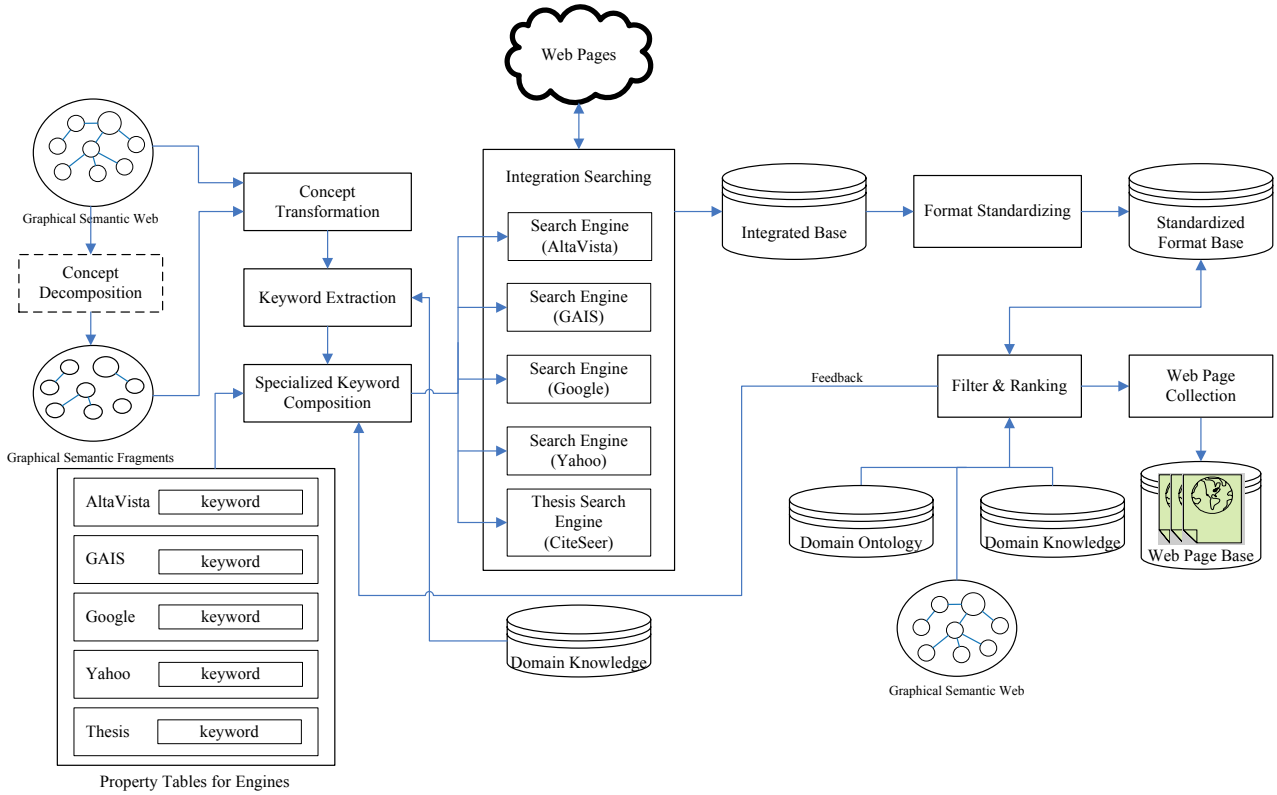
・filter & ranking

・web page collection

三、網路整合式搜尋引擎機制

1. 前處理機制

前處理機制乃以本子計畫所提出「圖形化語意網」之相關研究為基，利用其所建構之關鍵字將其組合成有意義之字組，並依據網路上各家搜尋引擎之特定格式之要求，轉換成符合搜尋引擎之 URL 逕行網頁搜尋，其步驟如下：



圖一　網路整合式搜尋引擎機制架構

(1) concept transformation：將經由圖形化的語意網輸入至 concept decomposition mechanism，主要功能是把完整圖形化語意網進行分割的動作，將分成多個有意義的子概念。此工作是為避免完整的概念於網路上無法找到符合的結果。因此搜尋的工作包含兩者：一是將整體圖形語意網及完整的概念傳遞到本研究所選定的四具著名搜尋引擎(AltaVista、GAIS、Google、Yahoo)進行相關網址的搜尋；二是以 concept decomposition mechanism 切割後的子概念稱之為「graphical semantic fragments」進行搜尋，之後將欲進行搜尋的概念轉成句子。

(2) keyword extraction：針對(1)的第二部份進行關鍵字擷取。主要利用每個子概念所標註的數個關鍵字，轉化成句子型態時都附註其上，再經由擷取組合成有意義之字組，其他子概念依此類推。

(3) specialized keyword composition：依據每個搜尋引擎的特性或屬性特徵，製作內含關鍵字組的 URL，並直接自動地對提供搜尋服務之網頁伺服器進行搜尋動作。

2. 整合式搜尋機制

(1) integration searching：每個搜尋引擎開始進行搜尋，之後搜尋結果被置入integrated base，被儲存的欄位有包含搜尋引擎名稱、網址、關鍵字、標題、網頁原始大小、純文字大小、摘要及文件原始碼等資訊。表一則為本研究所整理的四個著名搜尋引擎比較表。

3. 後處理機制

後處理機制主要是針對搜尋後的資料給予一致性的格式，並透過比對及排序演算法且應用實體論(ontology)概念處理摘要中涉及同義詞部份，這是本研究重點核心，最終期望能獲取最符合使用者原意的網頁，以便知識萃取，其步驟如下：

表一　搜尋引擎比較表（資料來源：本研究整理）

	AltaVista	GAIS	Google	Yahoo!	
搜尋方式	以關鍵字查詢為主	以關鍵字查詢為主	以關鍵字查詢為主	以分類目錄瀏覽為主	
搜尋字數上限	中文 800 字 英文 800 字	中文無 英文無	中文無 英文 2048 字	中文無 中文 100 字	英文無 英文 100 字
搜尋格式	html、pdf、ppt、doc、xml、txt	htm、html、xml、txt	rtf、ps、pdf、xls、ppt、doc、txt	htm、html、pdf、xls、ppt、doc、xml、txt	
類似查詢	有	有	有	有	
自然語言查詢	無	有	有	無	
多國語言查詢	有	中文、英文	有	有	
欄位查詢	url	url	link、related	title、url	
刪除重複網址	無	無	無	無	
刪除無效連結	無	無	無	無	
刪除廣告	無	無	無	無	
搜尋引擎排名	全球第 1	台灣第 6	全球第 6	全球第 2	

(1) format standardizing：網路上的資料格式大多以 HTML(Hyper Text Markup Language)與 PDF(Portable Document Format)呈現且大都是非結構與半結構性，利用 XML 可達成結構化目的，XML 是一套資料的描述語言，主要是用來設計網頁中可攜帶結構化的資訊，並且允許使用者可以自行定義和它們文件相關的標籤，同時可透過自訂標籤、屬性、XML schema 與 DTD(Document Type Definition)[3][5]，來對標題與摘要進行定義成為所需格式，稱為

format standardizing，隨後儲存到 standardized format base。

(2) filter & ranking：將格式標準化的摘要與標題進行比對，主要依據 graphical semantic net 和 domain knowledge 所提供的知識為基準，計算每篇摘要的資訊含量，其計算公式如下：

$$R(i, j) = \frac{(U_i \cap U_j) * 2}{U_i \cup U_j} \quad [11]$$

$$S(i) = \sum_j R(i, j) \quad [11]$$

：中文詞彙

U_i ：所有句子 I 與句子 J 中相同的可比較單位

$U_i \cup U_j$

其中有四個比較法則：

- N 元詞只能與 N 元詞比對
- 標注詞只能與標注詞比對
- 每個詞只能比對成功一次
- 詞的比對不考慮順序性

若不符合的項目會自動刪除，剩下符合項目，稱為比對演算法(match algorithm)，演算流程如圖二所示，緊接透過個數與次數演算法(occurrence hit algorithm)與過濾超連結演算法(filter hyperlink algorithm)進行更精密的過濾。這兩個演算法的發展是下一階段的任務，其概念是：前者藉由計算 occurrence 與 hit 值來去除重複出現之 URL，後者則是透過 occurrence 與 hit 兩個參數之運算可剔除廣告，可獲得所需要的 URL，此後會依據領域實體(domain ontology)去計算資訊含量高的摘要權重值並註記於實體概念裡；本研究採取 Gruber 的定義：Ontology 是一種對某一個概念的詳細描述，包括對於概念、關聯、實體的描述[17]。

其後再針對資訊含量中等的摘要進行判斷，部份摘要是描述不同但意思相同可稱同義詞，所以可給予相等權重值，至於計算權重的法則有下列五點[8][9]：

- 頻率關鍵詞法：動詞與名詞是句子的核心部份，文件中每一個動詞與名詞皆視為重要詞彙，而詞彙的重要程度，則視該詞彙在文件中所發生次數多寡。
- 標題關鍵詞法：一篇文章的標題往往選取與主題相關的字詞所組合而成，因此出現在標題的字詞要給予較高的權重值。
- 位置法：一篇文章最重要的部分大部分位於文章的首句與末句；學者曾指出簡單的摘錄文件中的前 60、150 或 250 個詞彙，便達到了 90%以上的可接受度。
- 標籤線索法：超文件提供某些特殊標籤，如：斜體字、粗體字、底線與

大小寫字體，都可以呈現相關重要的訊息。

- 領域實體論法：句子是由詞彙所組成，但詞彙之間會存在特定關係；同義詞包含廣義上的相關詞與狹義上的同義詞，前者是指某篇摘要述敘不同，但意義與原意類似的詞；後者是指某篇摘要述敘不同，但意義與原意相同的詞，如：西瓜與蘋果同屬於水果；台灣最高執政單位是意指總統府等諸如此類關係，會善用已建立的領域實體架構，包含同義詞與延伸詞，設法從中條列出詞彙間的規則並計算彼此間的相似度，其公式如下：

$$Sim\left(W_1, W_2\right) = \frac{2 \times \left|S\left(W_1\right) \cap S\left(W_2\right)\right|}{\left|S\left(W_1\right)\right| + \left|S\left(W_2\right)\right|} \quad [10]$$

W_i：中文詞彙

$S(W_i)$：將中文詞彙W_i拆解成詞素，所得的詞素集合

$|S(W_i)|$：詞素集合 $S(W_i)$長度

其效能達到93.5%的應用率以及93.8%的正確率[10]，但上述的五準則乃需要依實際情況去做調整，才能進行權重之計算。至於權重之計算如下：

$$SCORE = \sum_{k=1}^{n} TP_k + PW + \sum_{l=1}^{m} T_l W_t + SW \quad [9]$$

：摘要中第k個詞彙的權重　n：重要詞彙總數

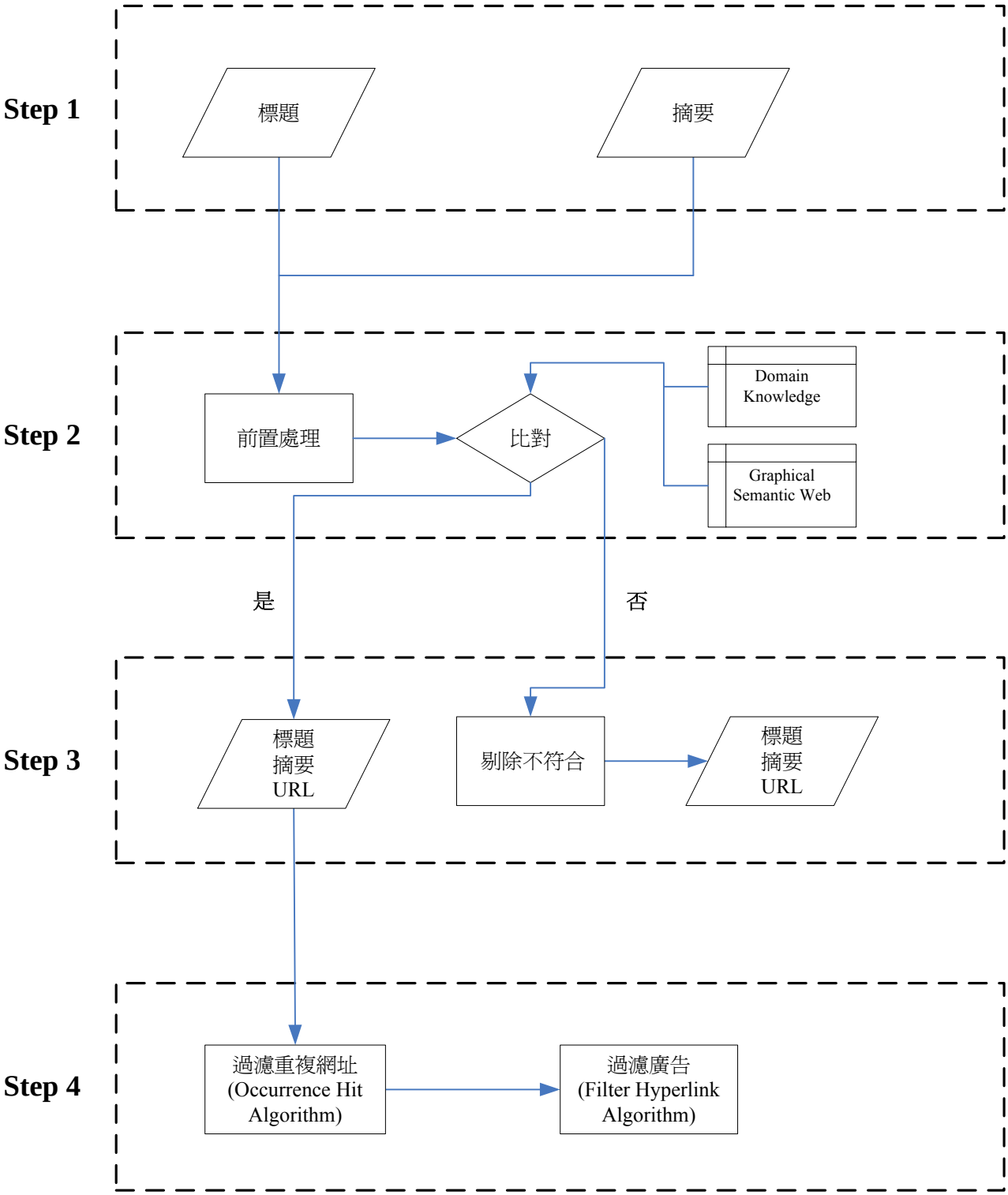
TP_k：位置權重　　：詞彙的標題與標籤權重　m：加權詞彙總數

PW：同義詞權重(Synonym Weight)　　TW　　：總得分

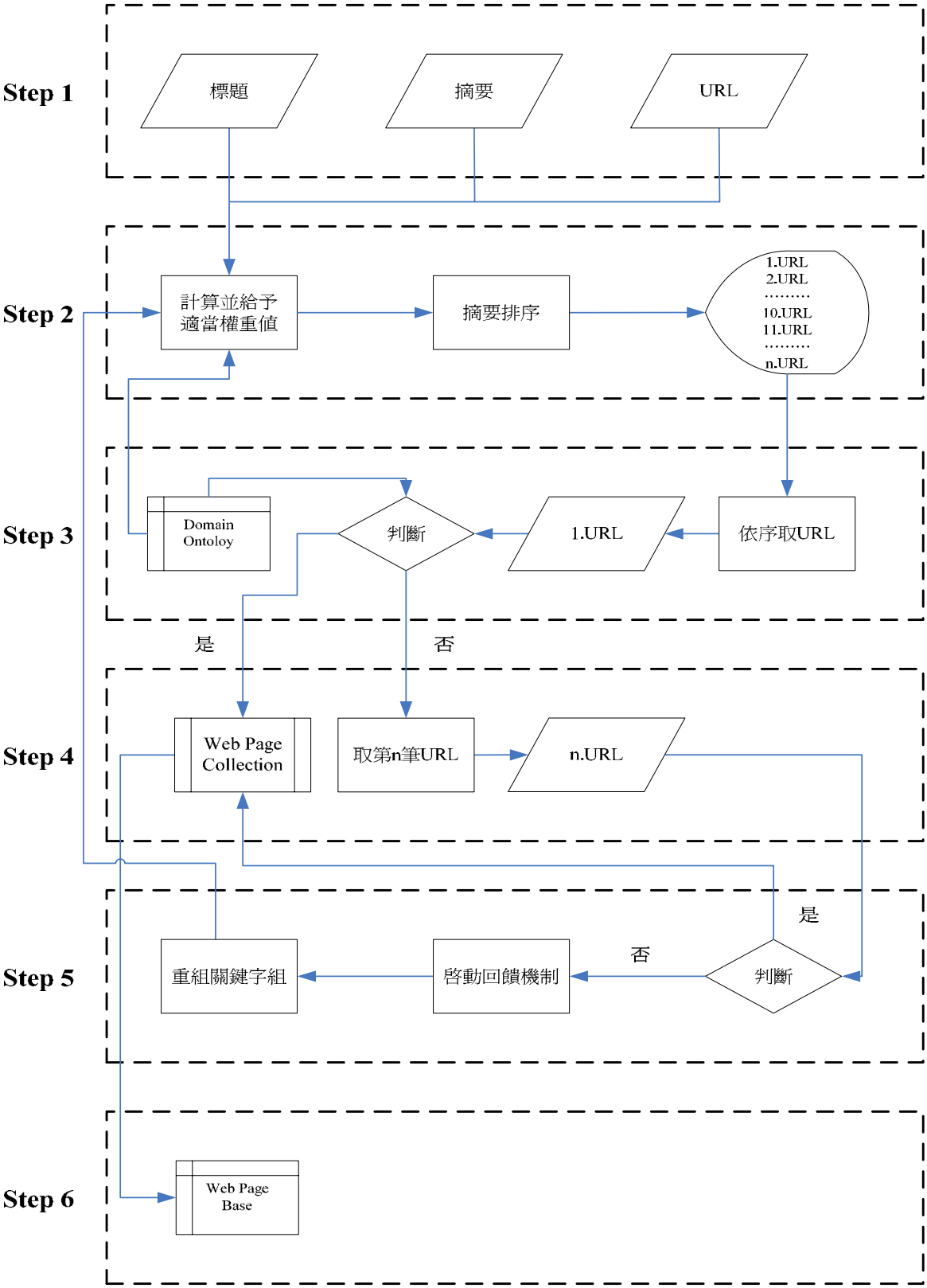
SW　　$SCORE$

摘要經計算後此處會設定適當門檻值，取出適合的部份並由高至低排序，接著依順序取一筆一筆資料與領域實體判斷是否符合其原意，若不符合再取第 n 筆資料來查看，若還是無較佳解立刻啟動回饋機制(feedback)返回 specialized keyword composition 並依前述的關鍵字重新組合，基本是依子概念中的數組關鍵字所組成，並排除重複性排列，採用關鍵字遞減方式來組合，如：有三組關鍵字分別為 a.國小、b.四則運算及 c.乘法，先利用三組字去組合關鍵字進行搜尋，若無解答則利用兩組關鍵字組合或單組關鍵字進行排列，再置入搜尋器中搜尋，其他依此類推繼續執行前面步驟，可稱為排序演算法(rank algorithm)，流程如圖三所示。

(3)web page collection：取回經由標準化與過濾等動作的實際網頁內容。


Step 1
標題
摘要
Step 2
前置處理
比對
Domain Knowledge
Graphical Semantic Web
是
否
Step 3
標題
摘要
URL
剔除不符合
標題
摘要
URL
Step 4
過濾重複網址
(Occurrence Hit Algorithm)
過濾廣告
(Filter Hyperlink Algorithm)

圖二　比對演算法流程



圖三　排序演算法流程

四、結論

目前各家搜尋引擎功能旗鼓相當，搜尋結果實際上差異性不大，重點能減少頻寬負載量，避免使用者浪費精神與時間自行過濾檢索。因此本研究提出一套整合型搜尋引擎及建構機制架構設計，透過分析判斷過濾與排序之整合型搜尋引擎機制及演算法，除去網頁空間早已不存在之URL，提供擁有統一格式、標題、內容大小與摘要的URL及其網頁，保證每則超連接都存在，使資料庫中的資訊負荷降至最低。網路上搜尋的摘要，通常是環繞著關鍵字呈現，可能是某篇文章開頭前十句話，導致無法找出網頁中所要的隱含知識，未來是否可用網狀結構圖形取代以關鍵字為主之搜尋，其結果有待評估，對格式標準化或許能嵌入更有意義的內容與標題，便於知識萃取。

由於前處理機制、整合式搜尋機制與演算法尚在積極進行中，未來預計提出其細部方法、步驟及實例。本研究之預期產出及貢獻如下：

(1)擁有關鍵字組合、格式標準化與過濾排序機制的整合式搜尋引擎。
(2)減少使用者搜尋時間讀取重複性太高的網頁且提高準確性與效能。
(3)提供較貼切原意的網頁給予使用者作為參考。
(4)資料文件利用 XML 技術達成一致性與結構化目的，有利於日後增減修改或傳遞，不會因為頻寬問題而損毀遺失。
(5)提出計算權重法則的領域實體論法，解決描述不同卻意義相同的摘要。

參考文獻

[1] Cooley, R., Mobasher, B. and Srivastava, J., "Web mining: information and pattern discovery on the World Wide Web," *9th IEEE International Conference on Tools with Artificial Intelligence (ICTAI' 97)*, 1997, pp. 558-567.

[2] Jenkins, C., Kackson, M., Burden, P. and Wallis, J., "Searching the world wide web：an evaluation of available tools and methodologies," *ELSEVIER Journal on Information and software technology*, 1998, pp. 985-994.

[3] Norman, Walsh, "A Technical Introduction to XML," *World Wide Web Journal*, 1998 (http://www.nwalsh.com/docs/articles/xml/).

[4] Spertusm, E., "ParaSite：Mining Structural Information on the Web," *The Sixth International World Wide Web Conference (WWW6)*, 1997, pp. 1205-1215.

[5] 王常威，『以內容為基礎之 XML 文件分類方法之研究』，2004，成功大學資訊管理研究所碩士論文。

[6] 陳麴合，『超連結與關鍵字頻分析之搜尋引擎研究』，2001，屏東科技大學資訊管理研究所碩士論文。

[7] 許志新，『分散式搜尋引擎之設計與實作』，1996，中正大學資訊工程研究所碩士論文。

[8] 邱立豐，『互動式概念查詢應用於網路文件自動摘要之效益』，2002，雲林科技大學資訊管理研究所碩士論文。
[9] 黃純敏、吳郁瑩，『網路中文文件自動摘要』，台灣區網際網路研討會TANET，1999，國立中山大學承辦。
[10] 柯淑津，『從詞網出發的中文複名詞的語意表達』，International Journal of Computational Linguistics and Chinese Language Processing，2003，pp. 93-108。
[11] 謝文泰、陳鈺文、張覆平，『以句子資訊量來產生文件摘要之模式』，財團法人資訊工業策進會。
[12] The AltaVista Search Engine, http://www.altavista.com/.
[13] The GAIS Search Engine, http://gais.cs.ccu.edu.tw/.
[14] The Google Search Engine, http://www.google.com/.
[15] The Yahoo Search Engine, http://search.yahoo.com/.
[16] The CiteSeer Engine, http://citeseer.ist.psu.edu/.
[17] Tom Gruber, Ontology Definition, http://www-ksl.Stanford.edu/kst/what-is-an-ontology.html.

附件(六) 領域本體論為基之網頁知識擷取機制設計

摘要

文字探勘(Text mining)結合資料探勘、自然語言處理與資訊檢索技術，使大量不具結構的文字資訊能經由電腦自動的分析歸納，目前主要的應用有自動分類、自動摘要、文件檢索及知識管理。其中一個重要的主題「文件分群(text clustering)」，經由電腦自動依照其文件內容的相關性分群，使能更精確地找到所需的文件。本研究著重於小學生數學學習障礙的問題領域，透過領域本體(domain ontology)的應用，幫助我們從搜尋引擎所尋找回的文章進行分類。由於領域本體能夠描述特定知識領域內相關的概念與關係，利用此種特性，本研究提出一種以新式的本體論為基的文件分群技術，以期能有效的協助知識管理者在電子文件達到正確分群的管理。本研究首先利用訓練的方式，分別求得領域本體內每一個概念的權重值。當一份網頁文件需要分群時，先經由文件前處理程序得到文件的詞彙集合，然後與領域本體中的概念進行比對，求得文件與領域本體的對應關係。之後藉由領域本體與自然語言處理的結合，把使用者所輸入的問句分析，找出文章中符合的段落回應給使用者，促進知識的分享與再利用。

關鍵詞：網頁探勘、文件分群、知識擷取、本體論

1. 緒論

近年來資訊技術蓬勃發展，由於網際網路盛行拉近了人與人之間的距離，所有的訊息在彈指間都可以傳遞到世界上其它任何角落，也由於資訊數位化的因素，造成大量的資訊充斥在隨手可得的網路世界中，許多電子文件的服務也與日俱增，要如何尋找、收集資料，然後整理、探勘為有用的資訊便顯得一門重要的學問，要有效的管理這些資料也因此顯得格外重要，電子化文件若透過有效的分群方式，將文件存放在適合的群組中便能夠有效的協助人們尋找需要的資料。

然而，透過人力將文件群聚往往耗時而且判斷上容易顯得不夠客觀，因為相同的文件由不同的人員來群聚可能會有差異，甚至相同的人員在不同的時間也可能對同一份文件做出不同的群組判斷，所以，自動化文件分群透過機器學習各群組中文文件之特徵，改善分群效果，又不需耗費大量人力，更重要的是能夠達到客觀性與一致性，因此自動化文件分群在知識管理或資訊檢索相關研究領域上算是相當重要的一種研究。

2. 系統架構與方法

2.1 智慧型網頁知識擷取架構

本研究將網頁探勘模組分析成三大塊部份：(1)圖形化語意轉換機制、(2)整合型搜尋引擎機制及(3)網頁知識擷取機制：

- 圖形化語意轉換機制：把使用者輸入的文字,透過圖形化語意機制，把輸入的文字進行圖形化的語意轉換,也就是說主要的目的在把描述的問題進行剖析，利用圖形化的方式把詞彙的同義字擴展出來成為語意網。
- 整合型搜尋引擎機制：把使用者輸入的問題經由圖形化語意轉換機制後，可得到詞彙的語意網，此語意網包含同義字且向外延伸詞彙與詞彙間關聯強度。搜尋引擎根據已知的語意網，根據詞彙的關鍵字透過四具搜尋引擎(yahoo, google, AltaVisa and GAIS)搜尋有關解決問題的網頁，然後再根據使用者輸入的問題比對出最符合的網頁，並且把格式轉換為 XML 形式。
- 網頁知識擷取機制：本機制利用在經由上述中所提出之整合式搜尋機制在網路上搜尋的結果來進行網頁內容的初步分析的工作。在這個階段包含有三個主要的活動，分別說明如下：

(1) **Clustering and Ranking**：首先將儲存在網頁庫(Web Page Base)中的已被標準化並以 XML 檔案格式儲存的網頁進行分群的工作，之後進行同類網頁的排序工作。為了將網頁適當的依專業領域自動的進行分群，本研究整合目前已

被提出之分群技術，提出一個分群的方法，這個方法的程序如下：

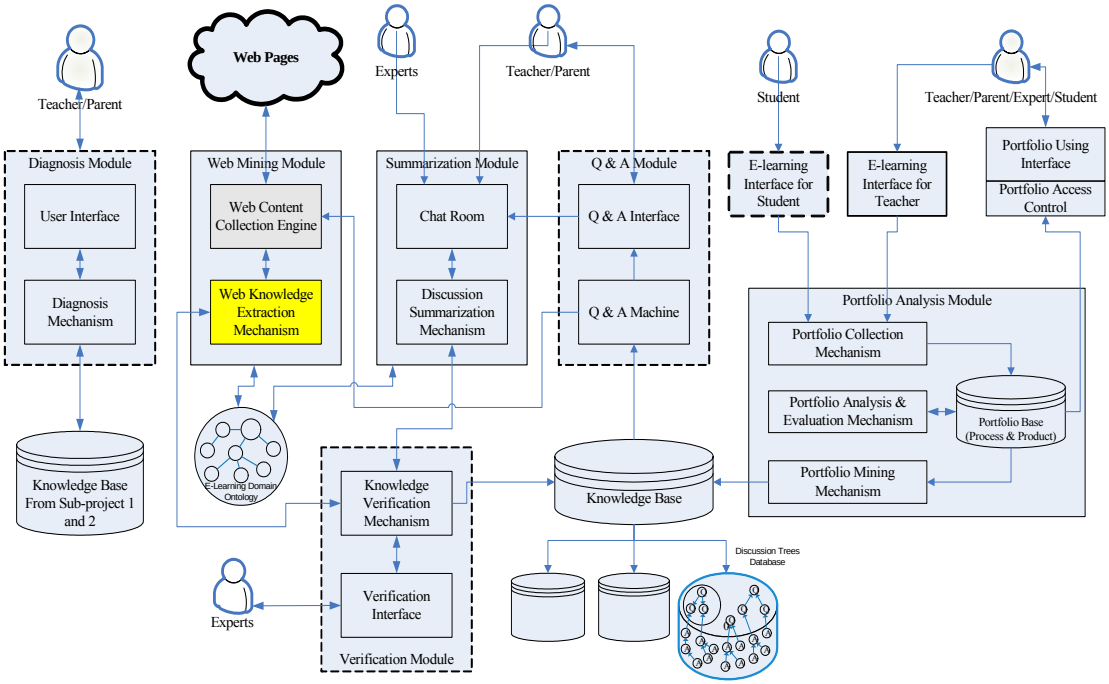
Step1：利用事先建好的 domain ontology 定義出每個 concept；

Step2：把每個 concept 看作成一個 term；

Step3：透過訓練集，利用 CKIP 處理訓練集，推斷出訓練集中常出現的詞彙；

Step4：建構出每個詞彙的 domain concept；

Step5：往後若有類似文章經過 CKIP 處理後，其 concept 若出現在訓練集中，則視為同一群組。



圖二:系統架構圖

Non-Ontology based Clustering Method：萬一字詞的未出現在 domain ontology 領域中，則採取以下的方法把文章分群：

1.若沒有建構 domain concept，則以 TF-IDF 計算出文章常出現字詞的權重。

2.計算每篇文章內容常出現的詞彙的權重，以 VSM(向量模式)比較相似度。

(2) **Content Extraction:** 經由標準化並以 XML 檔案格式儲存的網頁，XML 格式是由許多標籤所組成，每個標籤在 XML 中各有其意義，可標示由哪具搜尋引擎所尋找回來的網頁，也可標示文件大小或者文章簡述等等。透過搜尋

引擎機制中的自訂標籤格式，將網頁文章主體擷取出來。

(3) Content Decomposition:網頁文章是由各個段落組成，而各段落又是由句子所組成。在此步驟需先將網頁文章主體根據自訂標籤擷取出來後，針對內容的部分進行拆解。依據問號、句號等等拆解成為各個段落與句子。然後依照 TFIDF[12]與 Information gain[4][5]兩種方法，計算出關鍵字詞在每一個段落與句子彼此之間的重要性，以利於下一步驟「知識擷取機制」。

(4) 知識擷取機制：本研究所提出的「知識擷取機制」能在冗長的文章濃縮成為簡潔的摘要，省去使用者查閱網頁內容的時間，將濃縮的知識呈現給使用者。其主要機制說明如下：

Step1. Feature Extraction: 特徵擷取的任務在於減少資訊量，不重要的詞彙從特徵項空間中刪除，從而減少特徵項的個數。把網頁內容拆解成段落後，利用分號、句號、問號等等將段落分解成句子，並且儲存到 decomposed content base。計算關鍵字在句子中的權重高低，把權重突出的句子提取出來，進行排序與過濾的動作。

Step2. Ranking and Filtering: 給定門檻值後，把權重值過低的句子去掉，並且結合 domain 構詞規則與 domain knowledge，將句子與句子之間按照權重高低排序起來。

Step3. Knowledge Construction: 透過句子與句子之間和 domain 構詞規則後，則可以產出整篇網頁文章的知識，並且將這些知識總結。將權重值較高的句子依序排列，配合領域詞庫斷詞法、內文關聯法(Global Bushy Path，GBP)[6][7]來產生每一篇文章並可動態產生摘要，以兩百個字為預設值。

萬一動態產生的摘要並不如使用者所預期的知識，則本研究提出一個用來判斷文章中的段落是否能符合使用者語意的方法。此方法如下：

$$imp(p,D)=\frac{1}{|s|}\sum_{Keyword=1}^{N} weight(FW_1+FW_2+..+FW_N,D)$$

P：文章段落

D：網頁文章

|S|:段落中所有的名詞，也就是 Na、Nb、Nc 的詞頻

Keyword:經過 CKIP 處理過後分析出來的關鍵字

N:文章中關鍵字的總數

F:關鍵字出現的次數

W：利用 ontology 所建構出的權重值

希望透過此方法能找出文章中符合語意的最佳段落回應給使用者。

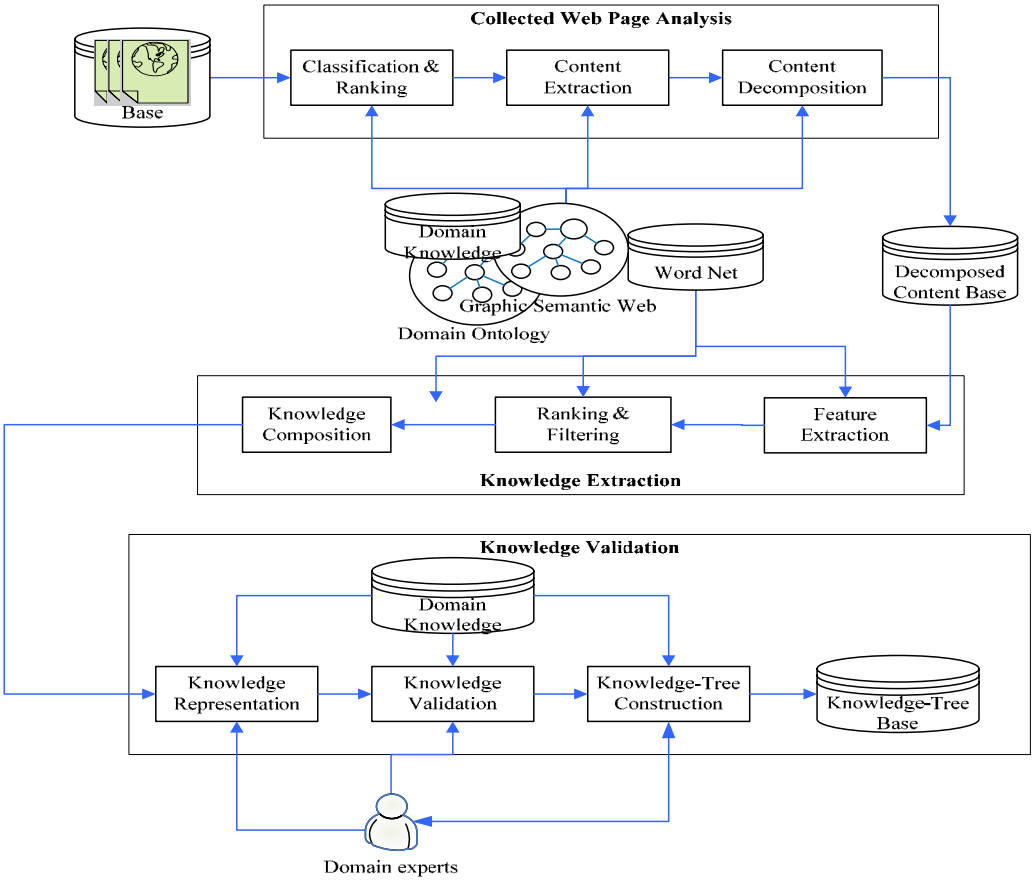
(5) 知識確認：當隱含在網頁的知識經過一連串的擷取程序形成摘要並組成知識之後，必須進行知識的呈現與知識的驗證的工作。知識驗證子系統的架構如圖三的下半部所示，其中包含幾個主要的元件，有：知識的展示、知識的確認及知識樹的建構，細部說明如下：

Step1. Knowledge Representation: 網頁的知識經過前述核心功能處理過後，可以把隱藏在網頁中的知識擷取出來，形成摘要並組成知識後，並且配合 domain knowledge 將摘要中意義不大或者較無相關的字詞去除，將簡潔的摘要知識呈現給使用者。

Step2. Knowledge Validation: 除了把隱藏於網頁中的知識擷取成為摘要後，還必須確保知識的準確性，因此透過領域專家針對每篇文章的摘要進行知識驗證，然後把領域專家判斷無誤的摘要輸出，作為建構知識樹的主要輸入來源。

Step3. Knowledge-Tree Construction: 把每一篇網頁文章摘要形成節點，節點中的檔頭標註網頁文章的標題，而其後面的標註為網頁文章摘要。計算往後每一個新進來的節點與根節點的相似度，然後再決定知識樹先後的走

訪順序。隨著每一次使用者所下的關鍵字詞經過網頁整合式搜尋引擎與網頁知識擷取機制後，節點會越來越多，此時把知識樹的節點結構編碼成霍夫曼樹形式(Huffman Tree)，並且儲存至知識樹的資料庫中。在此編碼成霍夫曼樹是為了日後節點越來越多的時候，利用節點編碼可清楚了解摘要的編號。未來如果使用者對於當前文章擷取過後的摘要不甚滿意的時候，透過霍夫曼樹形式，計算當前的節點與知識樹資料庫中的節點兩者相似度，提供使用者當前節點裡面的摘要與以往類似文章節點的摘要，兩兩比較。若類似的文章使用者仍不滿意，則繼續透過霍夫曼樹形式找出第二相似者，依此類推形式，以期望滿足使用者求知的需求。



圖三: 網頁知識擷取機架構圖

3. 結論與未來發展

在此篇研究中，我們利用 ontology 技術，提出一個基於 ontology 架構的文件分群方式。利用 ontology 描述特定知識領域與清楚表達物件間的關係進而輔助分

群與產生摘要。首先我們將待分群的中文文章透過文件的前處理取出中文文件內的詞彙集合，接著建構出每一個詞彙的 concept，並且利用 concept 與 concept 之間的關聯性增加網頁文章分群的準確性。

由於本研究的分群方式需自行定義 ontology 的架構，隨著 ontology 的擴張，分群的效果也會更加精準。但是目前自動建構 ontology 的技術還不完善，尚無法建構更貼切符合專業知識領域的 ontology，因此在建構上還是需要耗費人力與時間，若是能夠自動建構與擴張的方法改善 ontology，則可以有效率的加強分群的準確性。

本研究的預期貢獻有以下幾點：

1.提出一個以多個關鍵字來評斷文章段落是否符合語意的方法。

2.透過 ontology 的建構技術，提出一個基於 ontology 架構的文件分群方式。

參考文獻

[1] Web Mining Books - Morgan Kaufmann, “Mining The Web-Discovering Knowledge From Hypertext Data,” 2003.

[2]Dragos Arotaritei，Sushmita Mitra,web mining :a survey in the fuzzy framework

[3]Sung Ho Ha,Sung Min Bae,Sang Chan Park,web mining for distance education

[4] Tatsunori Mori., “Information Gain Ratio as Term Weight-The case of Summarization of IR Results,” In Proceedings of the 19th International Conference on Computational Linguistics, pp688-694, 2002.

[5] Tatsunori Mori., Miwa Kikuchi., and Kazufumi, Yoshida Term “Weighting Method based on Information Gain Ratio for Summarizing Documents retrieved by IR systems,” In Proceedings of NTCIR Workshop 2 Meeting, pp5-205-5-212, 2001.

[6]黃純敏、楊存一、邱立豐，國立雲林科技大學資訊管理研究所；TFIDF 觀念於自動摘要評估

[7]黃純敏、楊存一、邱立豐，國立雲林科技大學資訊管理研究所；中英文網路文件自動摘要之研究

[8]廖嘉欣，「實體論自動建構技術與其在資訊分類上之應用」，成功大學資訊工程學系碩士論文，91 年 7 月。

[9]鐘明強，「基於 ontology 架構之文件分類網路服務研究與架構」，成功大學資訊工程學系

碩士論文，93 年 7 月。

[10]郭家良，「新聞事件群聚及摘要檢索研究」，雲林科技大學資訊管理學系碩士論文，93 年 6 月。

[11]王美淳，「利用共生詞彙特性發展一個二階段文件群集法」，中原大學資訊管理學系碩士論文，92 年 5 月。

[12]黃佳新，「關鍵字擷取與文件分類之因子分析」，清華大學工業工程系碩士論文，93 年 6 月。

附件(七)

Development of an Access Control Model, System Architecture and Approaches for Resource Sharing in Virtual Enterprise

Tsung-Yi Chen, Ph.D. Candidate[1], Lecturer[2]

Yuh-Min Chen, Professor[1]
Hui-Chuan Chu, Assocaite Professor[3]
Chin-Bin Wang, Professor[4]

[1]Institute of Manufacturing Engineering
National Cheng Kung University
Tainan, Taiwan, ROC

[2]Department of Electronic Commerce Management
Nan Hua University
Chia-Yi, Taiwan, ROC

[3]National University of Tainan
Tainan, Taiwan, ROC

[4]Dept. of Information Management
Nan Hua University
Chia-Yi, Taiwan, ROC

Corresponding Author:
Yuh-Min Chen, Professor
Institute of Manufacturing Engineering
National Cheng Kung University
Tainan, Taiwan, ROC
Email:ymchen@mail.ncku.edu.tw
TEL:886-6-2757575 ext. 63922
FAX:886-6-2085334

Development of an Access Control Model, System Architecture and Approaches for Resource Sharing in Virtual Enterprise

0. Abstract

Secure information sharing is one of key factors for success of virtual enterprise (VE). The study identifies the characteristics of a VE and analyzes the requirements of a VE access control. A Virtual Enterprise Access Control (VEAC) Model is proposed to handle resource management and

sharing across each participating enterprise, which consists of a Project-based Access Control (PBAC) sub-model to manage public resources and a Role-based Access Control (RBAC) sub-model to manage private resources. The architecture of a VEAC Model-based system is developed and consists of three core mechanisms including the Virtual Enterprise Access Control Center (VEACC), Security Gatekeeper (SG) and Global Certificate Authority Center (GCAC). Based on the system architecture, the study proposes certificate authentication, user authority and access control approaches to identify user's identity on-line, update and search user authority lists, and access private and public resources. The results of this study will facilitate more secure resource sharing, and overcome cooperation barrier from trust among participating enterprises in VE.

Keywords: Virtual enterprise, Information sharing, RBAC, Access control, Certificate authority.

1. Introduction

Virtual enterprise (VE) is a network of independent, geographically dispersed administrative business domains that cooperate by sharing business processes and resources across enterprises to provide a value-added service to customers. VE is treated as one of the most promising business strategies for enterprises to meet global competition [1, 2]. VEs integrate the processes, activities and resources from different enterprises through enterprise alliances to rapidly respond to customer expectations. In practice, a VE is implemented with a distributed and collaborative business process, in which individuals from different enterprises cooperate on business-related activities or processes through remote coordination, communication and control [3, 4].

Real-time information sharing and resource management within a manufacturing-based company or across companies are essential in the era of internet. For instance, a new automobile model is developed by a virtual enterprise that involves approximately 20,000 designers and engineers from hundreds of divisions and departments, some of which are in different enterprises in different countries. A virtual enterprise can be comprised of several sub-VEs. In the above example, one of sub-VEs in the VE to perform product design involves four sub-projects: Engine Design, Cool System Design, Transmission Case Design and Framework Design. The engineers of Engine Design sub-project design an engine for the new automobile model collaboratively. Information related to the engine design must be shared real-time to related engineers in the sub-project or other projects. Owing to the decentralized and dynamic characteristics in virtual enterprise environments, the success of a virtual enterprise heavily relies on full information transparency and correct resource sharing, including information, application systems and knowledge throughout the business cycle [4]. Even though the resource sharing leads to security and authority management problems, the issues of information delay and promote information transparency are still required to solve among business partners. The levels of resource sharing depend on characteristics of the VE, such as cooperative relationships with partners, depth of trust, functional tasks and contractual agreements. Access control and sharing for resource is most complicated in a virtual enterprise involving

cross-organizational activities. There must be security and audit measures to ensure that resource is legally used for the purpose intended by virtual enterprise.

The earliest access control models for resource sharing include ACLs (Access Control Lists) and ACMs (Access Control Matrix). These schemes are simple and intuitive, but are only useful for small organizations [5]. Most current access control policies, such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-based Access Control (RBAC) [6-9], Task-based Access Control (TBAC) and Task-role-based Access Control (T-RBAC) [10-12], consider merely the authorization management within a single organization. Some researchers have studied distributed role-based access control to delegate administration to individual departments in an enterprise [13]. TMAC04 (Team-Based Access Control 2004) was built on the RBAC, which allows users to join team roles in an organization [14]. Park *et al.* proposed a composite role-based access control approach that separates organizational and system level role structures to support scalable and reusable RBAC models [13, 15]. Cohen presented the family of CBAC (Coalition-based Access Control) models and policies to share specific data and functionality with coalition partners [16].

Although role-based methods have been successfully used in resource management within an enterprise, there are still many issues on management of resource sharing across organization boundaries to support collaborative and cooperative business activities. Access control for virtual enterprising is complicated because (1) members of the VE may change frequently; (2) VEs have members with complicated relationships; (3) VEs may be integrated or distributed, and (4) VEs are Internet-based and heterogeneous [17-23]. The goal of this study is to provide a solution for information sharing across enterprises to facilitate cross-enterprise collaboration and concurrency, and thus enable the above-mentioned difficulties to ease.

This study proposes a Virtual Enterprise Access Control (VEAC) Model to solve the problem of authorization management and security control among organizations within a VE. The proposed model consists of a Project-based Access Control (PBAC) Model for managing *public resources* within VE and an RBAC Model for managing the sharing of an individual enterprise's *private resources* with VE members. The architecture of a VEAC Model-based system is developed and consists of three core mechanisms. Based on the system architecture, the study proposes certificate authentication, user authority and access control approaches to update and search user authority lists. Besides resolving the issues of resource sharing across organizations, the following properties of the proposed access control model make flexible, adaptable, extensible and instantaneous at a minimum administrative cost: (1) the model enables resource managing and sharing collaboratively, (2) the model enables change of access rights dynamically, (3) the study prevents to disclose business secret in VE, and (4) the access authorization may be extended to the partners of the VE members.

2. Requirement analysis for access control in VE

The characteristics of a VE are identified by analyzing its life cycle and member interactions.

(1) A VE may consist of several distributed VEs or enterprises.
(2) A VE's participating members and business processes in a change during its life cycle.

(3) A VE emphasizes professional division and dynamic cooperation among a highly heterogeneous membership.

(4) A VE conducts business processes across enterprises divided into different stages, in which each stage has its own participants, resources and aims.
(5) In a VE, various resources are shared and distributed over all participating enterprises and used by their employees (users).
(6) A VE globally specifies members' obligations, responsibilities and roles.
(7) A change in a member's role in a process should not affect the obligations and responsibilities in its other assigned roles.
(8) Regulations do not constrain the selection of members in participating enterprises' partners.
(9) Each member may own its enterprise resource management policy and access control model.
(10) Shared VE resources include private resources owned by a participating enterprise and stored in its own repositories, and public resources belonging to the VE and stored in a public repository.

Based on the general requirements in access control in [10, 11, 16, 17, 20], this study identified the following requirements for access control model design: (1) only the security administrator is allowed to change security attributes; (2) roles may inherit authority either fully or partially); (3) the model supports active and passive access control, as well as the principle of strict least privilege; (4) the fine-granted authority requirements are fulfilled; (5) access authority may vary with tasks or roles, and (6) the model can manage all users and resource objects in the enterprise [17, 28, 29].

Besides the above requirements, based on the characteristics of VE, additional requirements must be considered when developing a VEAC model, as follows:

(1) Since the organization structure of a VE is dynamic, access rights and resource objects can be changed in real time.
(2) The model considers all users' access rights, because resource administrators cannot predict who will access which resources in a VE.
(3) As a VE is formed to achieve a certain goal in a limited time frame, each VE has different goal and business processes. A VE is always conducted as a project. Therefore, project is an essential unit of access control.
(4) Since each enterprise has a legacy access control system, the VEAC model is easily integrated with various access control models or policies.
(5) The VE manages and shares resources collaboratively.
(6) To facilitate trust among enterprises, the access policy in VE is planned and managed together by administrators of all participating enterprises.
(7) The VE can maintain the consistency of policies and manage the conflicts between VE access policy and members' own access policies.

Because the VE emphasizes applications of Information Technology and Network across enterprise boundaries, the following system-related factors are considered when developing a VEAC-based System:

(1) System must offer a gateway to access resources on distributed heterogeneous platforms must be offered.
(2) For high runtime efficiency, the access control system must be able to interact directly with other applications or agents.
(3) Users' identity must be authenticated via a third party called a Certificate Authority (CA) Center due to the issues of authentication and non-repudiation.
(4) To support integrity and confidentiality for information exchange, a Public Key Infrastructure (PKI) is needed.
(5) A flexible security system needs a Plug-and-Play key component to mediate between the VEAC Model and other RBAC-based Models.

3. Virtual enterprise access control model

Each participating enterprise may already have adopted an access control model before joining a VE. Therefore, the VEAC model must be able to integrate with other access control models. As RBAC is the most popular access control model [19, 30], the proposed VEAC model consists of a PBAC sub-model which can integrate into various role-based access control sub-models. This section presents and describes the two sub-models.

3.1 Overview of the concept

A VE's activities may use its own *public resources* of VE and the private shared resources of participating enterprises. Figure 1 illustrates the conceptual framework of the VEAC model in which the PBAC sub-model is designed to manage public VE resources, while the role-based access control model manages the private resources of participating enterprises. The VEAC framework primarily emphasizes on the following capabilities to resolve the problems of access control across enterprises: (1) The access control models of participating enterprises can be plugged-in or plugged-out at any time without affecting the performance of access control models in other participating enterprises; (2) The model can simultaneously manage public and private resources; (3) The basic information of models can be updated with changes in the environment to authorize new users; (4) The user authorities can be generated according to role hierarchy and relations; (5) The stratified management method is used to increase the security of public and private resources.

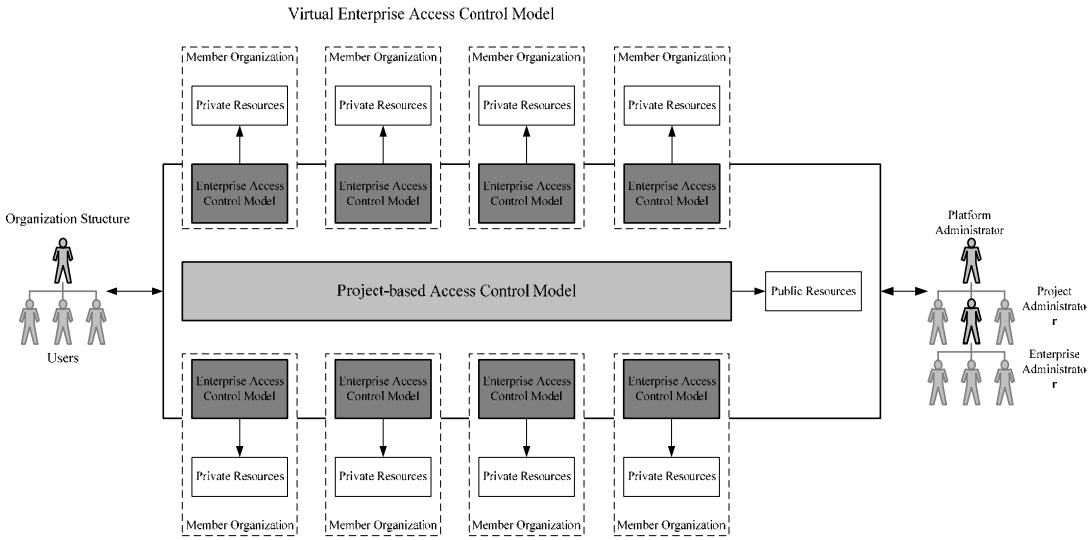


Fig. 1 Conceptual framework of VEAC Model

3.2 Role-based Access Control Model

This study slightly adjusted the RBAC model to seamlessly integrate it with the PBAC model. In the adjusted Role-based access control model, elements and assignments are simply described as follows:

- Users (U) represent a human or agent in an organization, which include direct users, indirect users, and non-member users.
- Roles (R) represent functional jobs or responsibilities.
- Private objects (PrivateO) represent resources in an enterprise associated with private privileges. Private Objects are usually classified into three levels including public, proprietary, and protection. The public classification can be provided to the partners in a VE.
- Private permissions (Private P) are approvals of a particular mode of access to one or more private objects.
- Sessions (S) represent each session, via which users are mapping to one or more roles;
- U-R-A $\subseteq$ U $\times$ R is a many to many user to role assignment relation.
- R-PrivateP-A $\subseteq$ R $\times$ PrivateP is a many to many role to private permission assignment relation.
- PrivateP-PrivateO-A $\subseteq$ PrivateP $\times$ PrivateO is a many to many private privilege to private object assignment relation.

3.3 Project-based access control model

This section elucidates the PBAC Model and defines all its elements, assignments among elements and assignments among models.

3.3.1 Core concept of the PBAC model

A "*virtual enterprise*" (VE) can perform several "*projects*" (P), but a project can only be performed by one VE. Different "project relations" (PR), such as subset, exclusion and reference, exist among projects. Activities within a project can be divided into several "*functional tasks*" (FT), each of which has access to certain public resources, which is their "*public permission*" (PublicP). A project involves some "*virtual enterprise roles*" (VER) to perform functional tasks.

A VE is composed of several real "enterprise members" (EM), each of which can participate in more than one VE. "*Non-enterprise members*" (NEM) are real enterprises that do not participate directly in the activities of VE but participate in the activities of an enterprise member which performs directly the activities of the VE. All VE participants, including three user types, are called "*users*" (U) which may play a different "*role*" (R) in a different "session". Each role has access to private resources, called a "*private permission*" (PrivateP). A superior role can inherit the privileges of inferior roles through "*role hierarchy*" (RH). The enterprise member plays a VE role through a user or role to obtain the privilege of sharing public resources in the VE and carry out practically the obligations a given VE role, and to achieve the VE goals.

"*Project access control policy*" is designed to identify the resource sharing rules in a project. Through constructing relations among projects and a project access control policy, users can share resources among projects. The rules of sharing can be modified at any time.

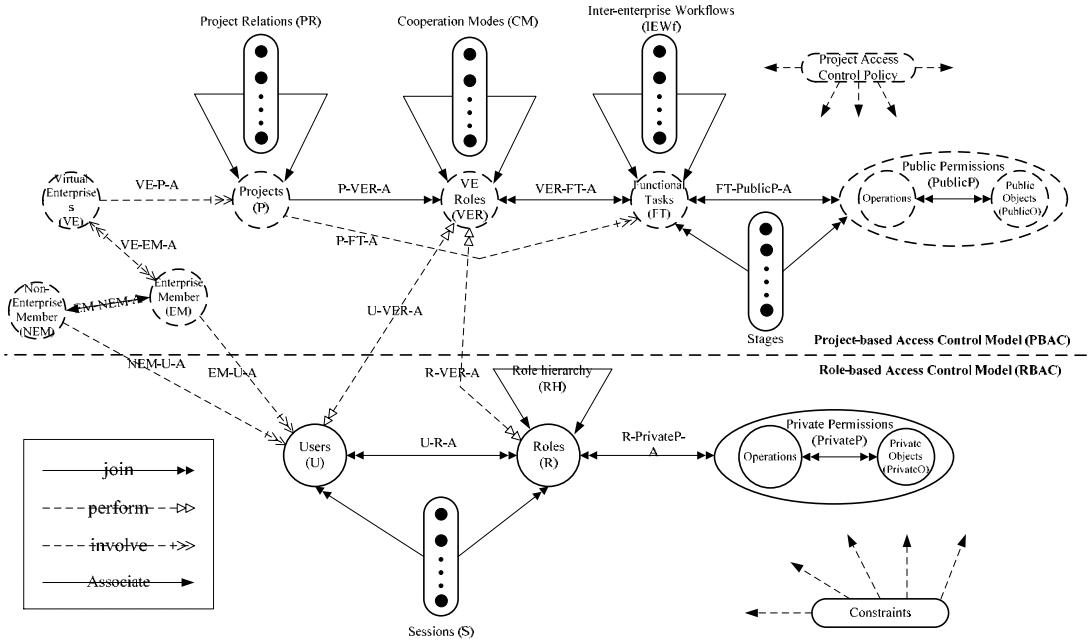


Fig. 2 Virtual enterprise access control (VEAC) model

3.3.2 Fundamental elements

This section defines all elements of the PBAC model:

- *Virtual Enterprise* (VE): The VE is a dynamic Internet organization, consisting of enterprise members, to achieve a business goal.
- *Enterprise Member* (EM): An EM can be a substantive enterprise organization, VE or individual, and is a VE member, with at least one worker participating directly the VE activities, and responsible for playing at least one virtual enterprise role.
- *Non-Enterprise Member* (NEM): An NEM is a substantive enterprise organization, VE or individual, but not a VE member, and participates indirectly in VE activities. An NEM has at least one worker participating directly in activities of enterprise members, and the activities have direct relations with functional task of VE.
- *Project* (P): A Project is the basic unit of VE activity. One project can have participants which are enterprises, departments or individuals, known as enterprise members. A project can be further divided into several sub-projects with various project relations. A project is composed of orderly functional tasks performed by enterprise members.
- *Functional Task* (FT): A FT is a set of VE activities which have a common objective to achieve a part of VE's responsibilities.
- *Virtual Enterprise Role* (VER): VERs, virtual roles created to enable professional divisions within VE, are the divisions of duties or activities in a VE, which are assigned to enterprise members to perform. Functional tasks can be assigned to one to more VERs.
- *Object* (O): Objects are the public and private resources held by VE and enterprise members. This study focuses on information objects, which can be databases, entities, attributes, tuples, documents, XML documents, applications, software components or knowledge.
- *Public Object* (Public O): Public objects are objects used by enterprise members and stored in a VE's common repositories. Public Objects are provided for performing functional tasks or are created when functional tasks are completed.
- *Private Object* (Private O): Private objects are a subset of objects owned by a VE's member and stored in a private repository.
- *Public Permission* (Public P): Public permissions indicate permitted modes of access to public objects.
- *Private Permission* (Private P): Private permissions indicate a permitted mode of access to a private object.
- *Permission*: Permission= $\{\text{PublicP} \cup \text{PrivateP}\}$.
- *Project Access Control Policy* (PACP): PACP identifies which project resource are protected and shared according to the relations among projects and the shared rules, and what activities are forbidden in the virtual enterprise scope. Each project involves a PACP which can be performed automatically by the VEAC system. The PACP can be dynamically created, enforced and adjusted when the VE environment changed.

3.3.3 Project relations

A Project Relation (PR) describes the interaction, cooperation modes and priority between two projects. Different project relations may exist between two projects and change with time according to project management requirements. In the VEAC platform, the administrators construct a relative project resource access strategy in project access control policy (PACP) to indicate the level of resource sharing of each type of project relations. In the project life cycle, the project relations and the PACP can be changed at any time to respond to demands of resource sharing.

(1) *Subset Relation* (PR_{subset}): Describes the relation between a "main-project" and its "sub-project". The subset relation is a binary relation. Several constraints are applied to use of subset relation: (a) a main-project may have more than one sub-project; (b) a sub-project may be involved in only one main-project; (c) an enterprise member may participate in the main- and sub-projects; and (d) a public permission may be merely assigned to different projects with subset relations. A main-project is allowed to access the resources of its sub-projects, but an administrator may set or disable the capability.

(2) *Version Relation* ($PR_{version}$): Describes a project "post-version project" which is extended from a project "pre-version project" and planned with reference to the pre-version project. Therefore, the pre- and post-version projects have similar targets, functional tasks and participants. The version relation between two projects may cause the correspondences between functional tasks of the two projects. The version relation is a binary relation.

(3) *Reference Relation* ($PR_{reference}$): Describes that a project "referring project" refers to the resources in other project "referred project". If the reference relation exists between two projects, the resources of referred project can be referred by users in referring project. The following constraints are applied when using the reference relation: (1) a project may set up more than one reference relation with other projects for resource sharing; and (2) a project may refer to various projects simultaneously.

(4) *Process Relation* ($PR_{process}$): Describes the executive sequence of two sub-projects from time perspective. It determines the time to sharing project resources. Expression $PR_{process}$*(event-project 1, …, event-project m; condition 1, …condition n; action-project k)* means that if event-project p_i for $1 \le i \le m$ is accomplished and condition c_j for $1 \le j \le n$ is valid, then action-project p_k can be triggered. When a project is decomposed into several sub-projects, Process Relation can be used to determine the executive sequence of all sub-projects. The process relation between two projects is a binary relation. While the relation is built on two projects, the administrator must specify the sequences of related functional tasks across project boundary. At the stages of executing an action-functional task which can use the resources of the event-functional tasks in event-project. The following constraints must be obeyed while using the process relation: (a) a process relation exists between two projects which must have the subset relation; (b) an event-project may trigger more than one action-project simultaneously; (c) an event-functional task may trigger more than one action-functional task simultaneously; and (d) an action-project may be triggered if all of its event-projects are accomplished.

(5) *Exclusive Relation* ($PR_{exclusive}$): Identifies mutual conflict between projects, so that the resources of the two projects cannot be referred to each other. The exclusive relation is

default. That is, if no other relation exists between two projects, then two projects are pre-set as Exclusive Relation. The exclusive relation is a binary relation. Supposing two projects are exclusive, then all functional tasks in a project are exclusive with the other project. The following constraints must be obeyed while using the process relation: (a) a project may conflict with more than one project simultaneously; (b) a public permission may not be assigned to two exclusive projects; and (c) an enterprise member is not allowed to be assigned to two mutual exclusive projects.

Figure 3 shows an air force bomber project as an example. Project 1.1, "aircraft structure" is, decomposed into four Sub-projects: Project 1.1.1 "fuselage", Project 1.1.2 "wings", Project 1.1.3 "tail", and Project 1.1.4 "landing". The schedule of Project 1 "air force bomber" in order is: Project 1.1 "aircraft structure", Project 1.2 "propulsion systems", Project 1.3 "aircraft control systems" and Project 1.4 "armament systems". The relation between Project 1 and Project 2 is an exclusive relation. Therefore, any resources of the two projects will be not shared during their life cycles. Partial works of Project 1.1.2 "wings" and Project 1.1.4 "landing" must refer to design diagrams of Project 1.1.1 "fuselage" while a stage of structure design of the Project 1.1.2 and the Project 1.1.4 "landing" is performed by workers of the two projects.

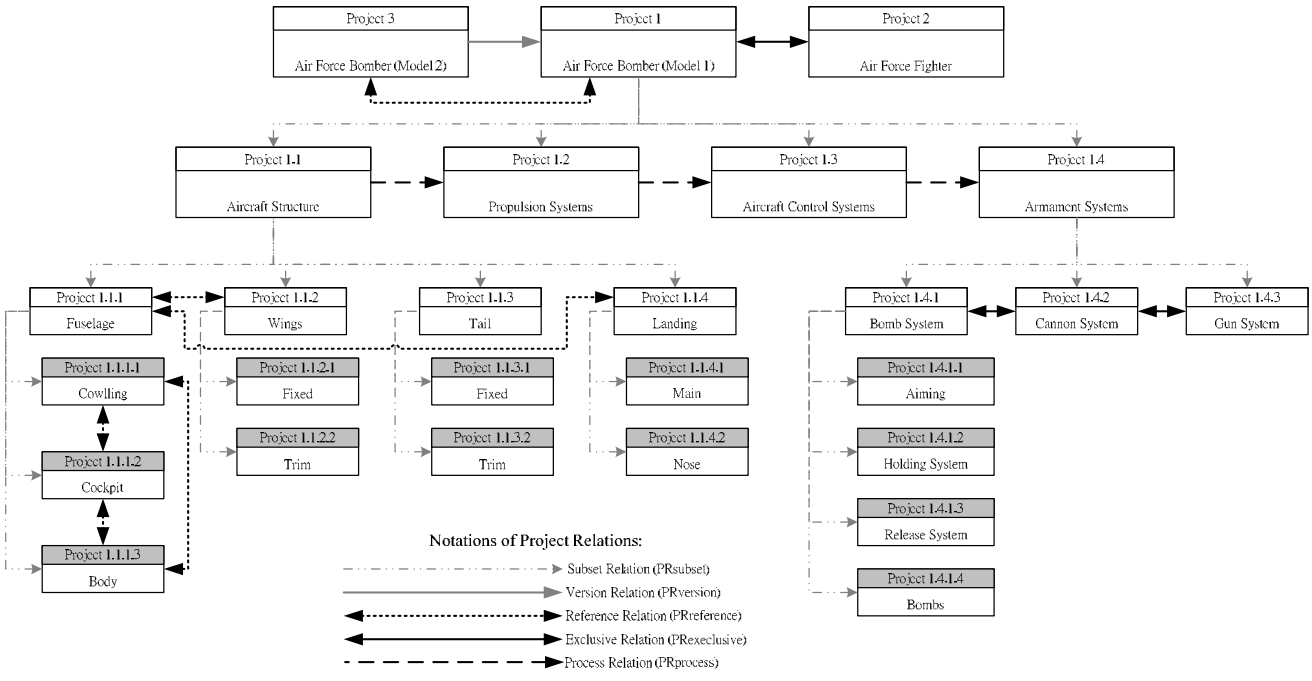


Fig. 3 Example of project relations

3.3.4 Cooperation Modes

This section presents three cooperation modes among virtual enterprise roles according to the resource sharing requirements of collaborative operations in the VE:

Cooperation Mode (CM) describes interactive method among virtual enterprise roles according to the dependence of their duties. The use of cooperation modes is constrained by the following rules:

(1) A virtual enterprise role is permitted to have different cooperation modes with other VE roles.
(2) Only one cooperation mode is permitted between two VE roles.
(3) The use of cooperation modes among virtual enterprise roles should consider the authority conflict problems caused by the reflexive, symmetric and transitive properties, as well as security problems caused by unlimited extension of permissions. The three above-mentioned properties of relations are discussed in detail in Section 3.3.5.

According to the VE coordination requirements, three cooperation modes exist:

(1) *Dependent Single-task Mode*: When several virtual enterprise roles cooperate to perform a functional task, they all have the same access privilege to all its resources.
(2) *Dependent Multi-task Mode*: Virtual enterprise roles perform related functional tasks separately. Outputs of the functional tasks are referred to each other.
(3) *Independent Mode*: Virtual enterprise roles perform independent functional tasks separately, disregarding their outputs. If two virtual enterprise roles work in an independent mode, then they may not have each other's access privileges for functional tasks performed by them.

3.3.5 Property of relations

This section presents a Role Relation Net (RRN) to identify the interactive relations among projects, cooperation modes, roles and hierarchical relations in enterprise members, assignment relations between users and roles and relations between roles and VE roles. Through the RRN, users can be authorized proper privileges in proper time according to roles played by users and VERs performed by roles.

Figure 4 shows an example of an RRN. The RRN includes two projects, Project P1 and P2, performed by virtual enterprise VE1 and VE2 respectively. The members of VE1 involve enterprises E1, E2 and E3, while the members of VE2 involve enterprises E1, E3, and E4. Role R21 in enterprise E2 is responsible for playing VE role VER12 in VE1. Through the cooperation mode CM12 between VER12 and VER11, Role R21 can be authorized to use part of VER11's resources. Through the role relation RR12 between role R21 and R22, R22 is allowed to access part of VER12's resources of in VE1.

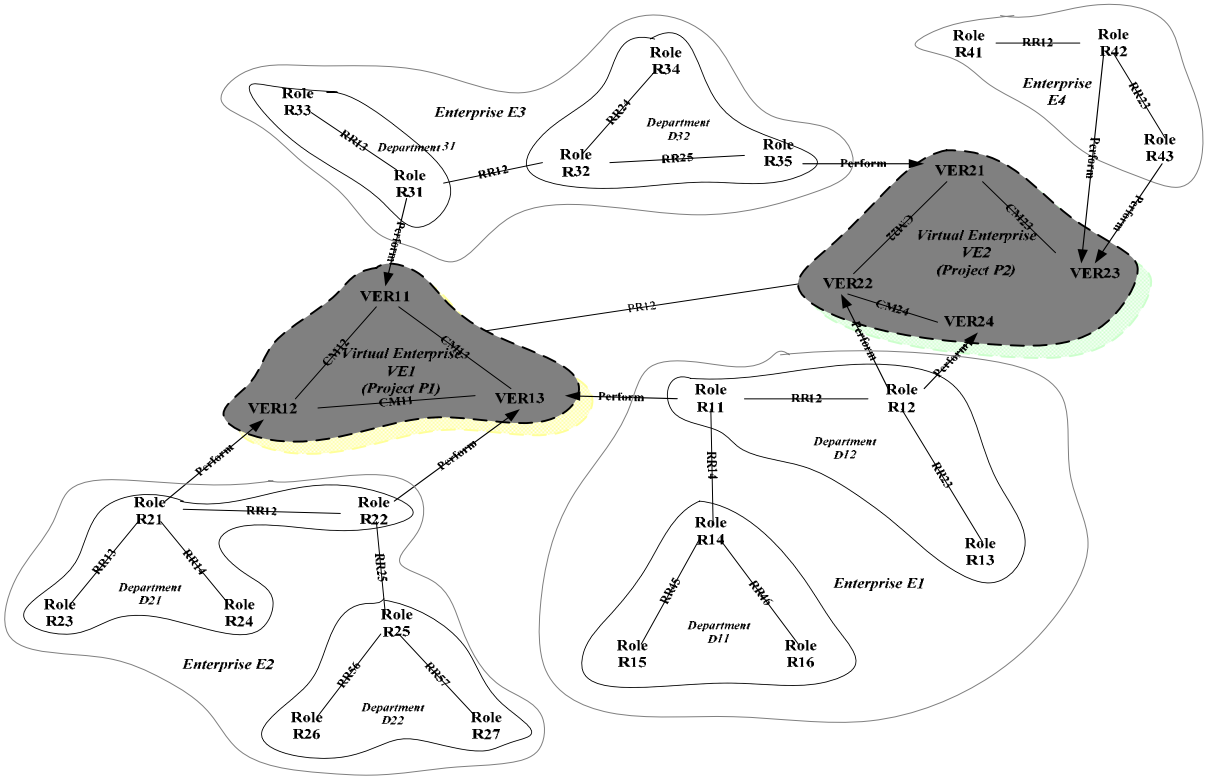


Fig. 4 Role Relation Net (RRN)

To avoid security problems caused by privilege expansion due to element relations, and to strengthen private and public resource security, three binary relation properties — reflexive, symmetric, and transitive — are applied to the above-mentioned relations.

In the project formation stage, members in a VE determine whether each cooperation mode and project relation satisfies these three properties. The enterprise itself can identify these three properties according to its own resource sharing rules. The enterprise can also set the depth of the transitive property and require symmetric and transitive properties to be valid only in the same department.

Tables 1, 2 and 3 list properties in project relations, cooperation modes and role relations respectively. Table 1 shows all possible combinations of the five project relations concerning reflexive, symmetric and transitive properties, which are introduced as follows:

(1) Subset Relation: The subset relation does not satisfy reflexive and symmetric properties. However, a project manager can determine whether the transitive property is satisfied. Meanwhile, the project manager can determine the continuability of the transitive property for resource sharing.
(2) Version Relation: The version relation does not satisfy the reflexive and symmetric properties, while the project manager can determine the transitive property. Meanwhile, the project manager can determine the continuability of the transitive property according to demands.
(3) Reference Relation: The reference relation does not satisfy the reflexive property because a

project does not need to refer to itself. However the project manager can determine whether the symmetric and transitive properties are satisfied according to demands. Meanwhile, a project manager can determine the continuability of the transitive property according to demands. If the symmetric property exists between projects p_1 and p_2, project p_1 refers to project p_2, and vice versa. If the transitive property of reference relations exists among projects, and project p_1 refers to project p_2 and project p_2 refers to project p_3, then project p_1 can refer to project p_3.

(4) Process Relation: The project manager may determine whether the reflexive, symmetric and transitive properties are satisfied.

(5) Exclusive Relation: The exclusive relation does not satisfy the reflexive property, while the project manager can determine whether the symmetric and transitive properties are satisfied.

Table 1. List of Project Relation Properties

Project Relation (PR)	Reflexive	Symmetric	Transitive
(1) Subset Relation	X	X	O(Degree) / X
(2) Version Relation	X	X	O (Degree) / X
(3) Reference Relation	X	O / X	O (Degree) / X
(4) Process Relation	O / X	O / X	O (Degree) / X
(5) Exclusive Relation	X	O / X	O (Degree) / X

Table 2 lists the three cooperation modes showing all possible combinations of their reflexive, symmetric and transitive properties. Since these properties have the same value, only the Dependent Single-Task Mode is explained. The Dependent Single-Task mode does not satisfy the reflexive property, but certainly satisfies the symmetric property because VE role ver_1 has cooperation relations of Dependent Single-Task Model with ver_2. Conversely, ver_2 has cooperation relations of Dependent Single-Task Mode with ver_1. Additionally, the project manager may determine whether transitive property and depth of transitability are satisfied.

Table 2. List of Cooperation Mode Properties

Cooperation Mode (CM)	Reflexive	Symmetric	Transitive
(1) Dependent Single-task Mode	X	O	O (Degree) / X
(2) Dependent Multi-task Mode	X	O	O (Degree) / X
(3) Independent Mode	X	O	O (Degree) / X

Table 3 lists role hierarchical relations, showing all possible hierarchical relations among roles, concerning their reflexive, symmetric and transitive properties. The properties of role hierarchy should be determined by the resource sharing strategy of an enterprise or department. Therefore, the Role hierarchy does not satisfy the reflexive and symmetric properties, but it is permitted to have different transitive properties among departments in the same enterprise. The depth of a role hierarchy's transitive property can also be determined, and the validity of transitive property may be established only within a department.

Table 3. List of Role Hierarchy Properties

Role Hierarchy (RH)	Reflexive	Symmetric	Transitive
Role Relation Name	X	X	O ($_{\text{Degree/Dep.}}$) / X

The properties of listed relations primarily have three effects: (1) To enhance resource sharing flexibility among projects and the availability of resource sharing in a VE; (2) To analyze whether project relations violate listed rules and to discover conflicts; (3) To analyze RRN to generate a user's privilege according to listed contents.

3.3.6 Foundational assignments

This sub-section defines various assignment relations among elements as follows:

- *Functional Task-Stage-Public Permission-Assignment* (FT-S-Public-A): A triple assignment relation among three elements: Functional Task, Stage, and Pubic Permission. Public permissions are assigned to functional tasks in stages. The relation among them is: FT × Stage × Public Permission.
- *Project-Virtual Enterprise Role-Assignment* (P-VER-A): This relation records the assignment relation between projects and virtual enterprise roles, and describes which virtual enterprise roles are included in a project.
- *Virtual Enterprise Role-Functional Task-Assignment* (VER-FT-A): This relation records the assignment relation between virtual enterprise role and functional task, and describes which functional tasks are performed by which virtual enterprise roles.
- *Virtual Enterprise-Enterprise Member-Assignment* (VE-EM-A): This relation records assignment relations between a VE and its enterprise members.
- *Virtual Enterprise-Project-Assignment* (VE-P-A): This relation records the assignment relations between a virtual enterprise and its projects, and describes which project is performed by a virtual enterprise.

3.3.7 Assignments across models

This section defines the relation assignments across models to establish the combination relations of relevant elements among two access control models. They are:

- *Enterprise Member-User-Assignment* (EM-U-A): This relation records the assignment relations between users and enterprise members.
- *Non-Enterprise Member -User-Assignment* (NEM-U-A): This relation records the non-enterprise members for which a user works.
- *Role-Virtual Enterprise Role-Assignment* (R-VER-A): This relation records the assignment relations between roles and virtual enterprise roles.
- *User-Virtual Enterprise Role-Assignment* (U-VER-A): This relation records what VE roles a user may play.

4. Classification of user authorities

Initially, according to the sources of user's authorities, a user's authorities can be classified into two categories as shown in Fig. 5:

(1)*Public authority*: The authority of public resources, which is obtained from VE roles performed by user roles. The authority of public resources can be subdivided into authority held by user and authority held by role. Because the algorithms for generating authority held by user is included in the algorithms for generating authority held by role, this study explores only the authority held by role. Its sources can be subdivided into three types:

(a) *Public Authority from VER*: The access authority derives from virtual enterprise roles played by user's roles in an enterprise member. Since user's roles can play different virtual enterprise roles, these authority of virtual enterprise roles may derive from different projects.

(b) *Public Authority from Cooperation among VER*: The access authority derives from virtual enterprise roles that can not be played by user's roles. These authorities are obtained through cooperation modes among VE roles played by the user's roles and other VE roles leading to resource sharing.

(c) *Public Authority from PRs*: The access authority derives from resource sharing among projects.

(2) *Private authority*: Authority of private resources existing in enterprise members and obtained through user roles. This authority can be subdivided into five types:

(a) *Private Authority from Roles*: The access authority derives from user's roles.

(b) *Private Authority from RHs*: The access authority derives from hierarchical relations between the entering user's roles played and roles not played by him. These roles inherit partial authority of other roles with which they have hierarchical relations.

(c) *Private Authority from VERs*: A VE role can be collaboratively played by many roles. To reach the common goal for performing VE roles, roles may share part of their authorities to other collaborative roles. Therefore, the access authority derives partially from the authorities of other roles with which the role cooperates collaboratively to perform the VE role.

(d) *Private Authority from Cooperation among VERs*: This authority uses authorities owned by other roles, exists in private resource of enterprise and is obtained through the cooperation model of playable virtual enterprise role and other virtual enterprise roles.

(e) *Private Authority from PRs*: This authority uses authorities existing in private resources in other enterprises and obtained through project relations.

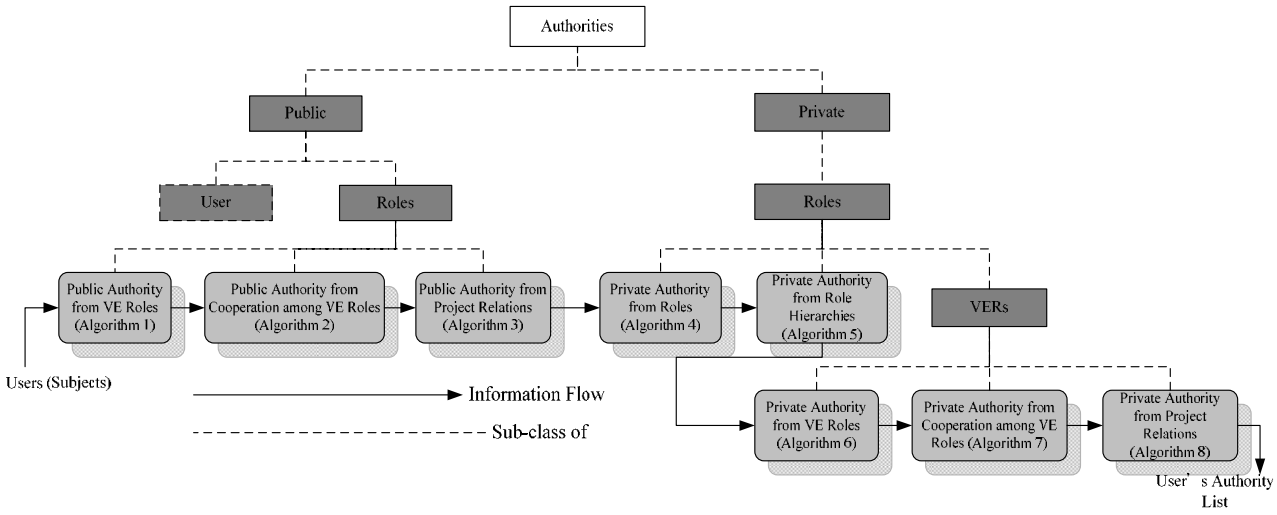


Fig. 5 Authority Classifications

5. System architecture and approaches design

To support resource management and security control in VE, this study developed a VEAC system based on the proposed VEAC model.

5.1 System architecture

This section designs the VEAC system architecture according to resource management requirements and characteristics in VE.

Figure 6 shows the VEAC system architecture, in which the primary mechanism includes a *Virtual Enterprise Access Control Center* (VEACC) responsible for authority management security control, and deployable in a leader enterprise. Every enterprise member joining the VE has to install a *Security Gatekeeper* (SG) to protect its own resources. To authenticate the user's identity on the Internet, the VEACC sends the user's login to the *Global Certificate Authority Center* (GCAC).

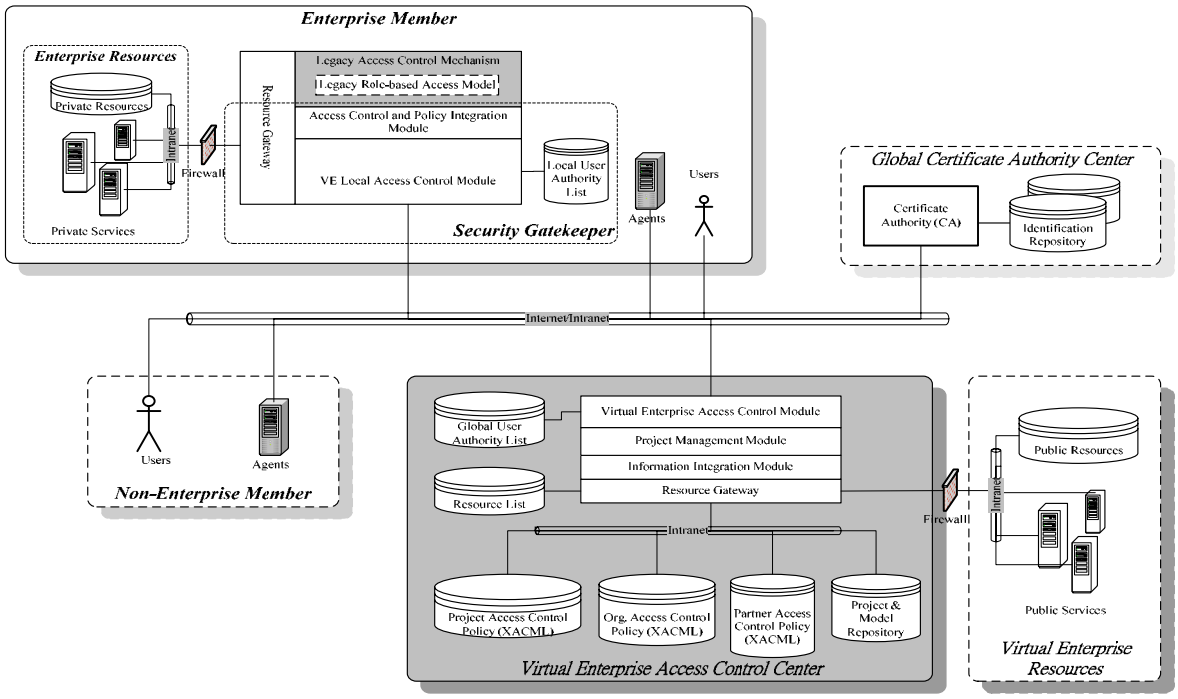


Fig. 6 A VEAC system architecture

The main mechanisms in the VEAC system architecture are introduced as follows:

- *Virtual Enterprise Access Control Center* (VEACC): The aims of the VEACC include: (1) to enable the administrator to construct and maintain systems; (2) to provide an interactive interface with other mechanisms, and encryption and decryption for secure communication; (3) to generate user authority lists according to the VEAC model; (4) to authenticate the user, and (5) to request resource services in the VE. Based on the aims and function requirements of virtual enterprise access control, a functional framework of the VEACC is designed as Fig. 7, which displays the main functional modules or components and their repositories. The functional framework of VEACC consists of the following modules:

(1) GUI user and administrator interface includes user requirement interface, team administrator interface, organization administrator interface and platform administrator interface;

(2) Model and policy integration module includes both model integration unit and policy translation unit;

(3) Authentication and access control module includes identification and authentication unit, policy handler unit, audit unit, session management unit, and access control and authorization unit;

(4) Information integration mechanism is able to transform various information into a understandable information format for users, and

(5) Resource gateway is an interactive interface to connect public resources and each member enterprise's security gatekeeper for accessing private resources through firewall.

These repositories in the framework are designed to store (1) resource list, (2) project and

model specification, (3) project access control policy, (4) intra-enterprise access control policy, (5) supplier access control policy, and (6) historical transaction data to support access control activities, including user's authentication and authorization, and examining disallowed accesses.

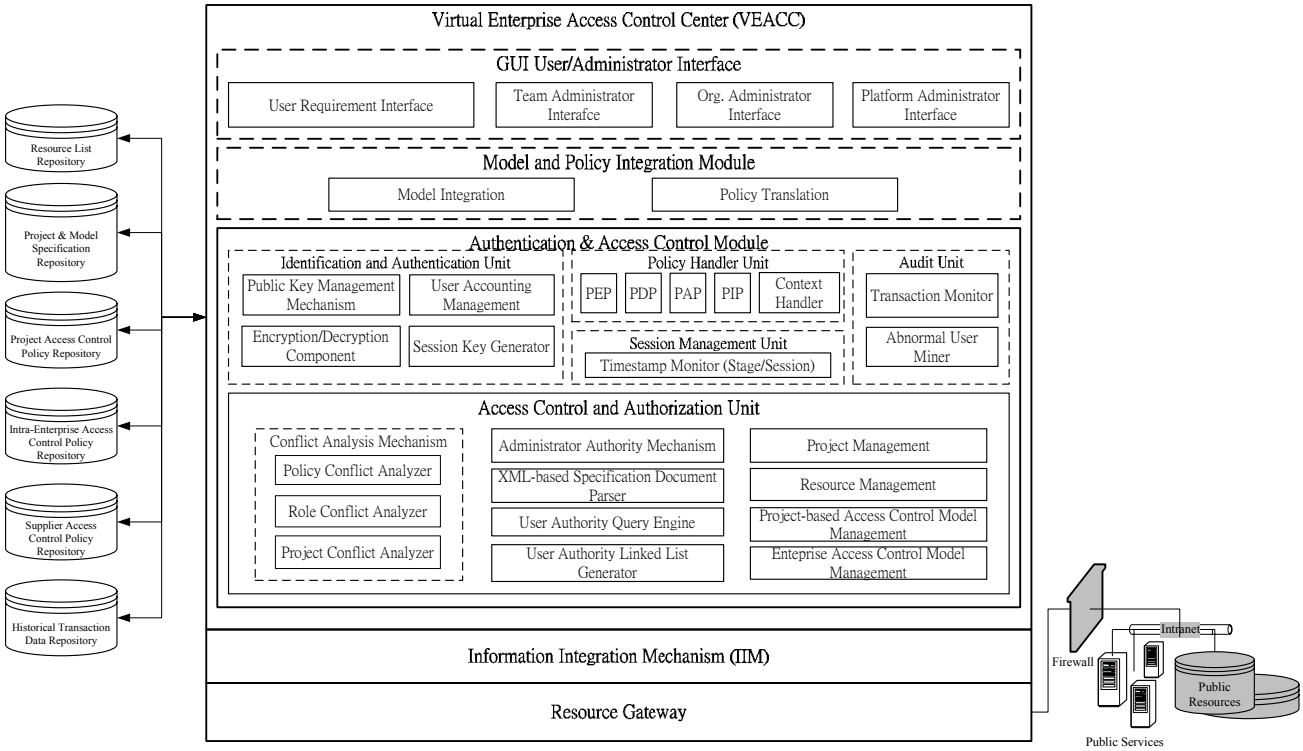


Fig. 7 Functional framework of VEACC

- *Security Gatekeeper* (SG): Every enterprise that joins VE has to install this component to (1) protect its own internal resources; (2) act as an interface for communicating with VEACC, and (3) request resource services in enterprises. The functional framework of security gatekeeper designed as Fig. 8 which consists of three main function modules: (1) virtual enterprise local access control module comprising local user authority manager, user authority checker, encryption and decryption component, and service requestor and receiver, (2) access control model and policy integration module, and (3) resource gateway.

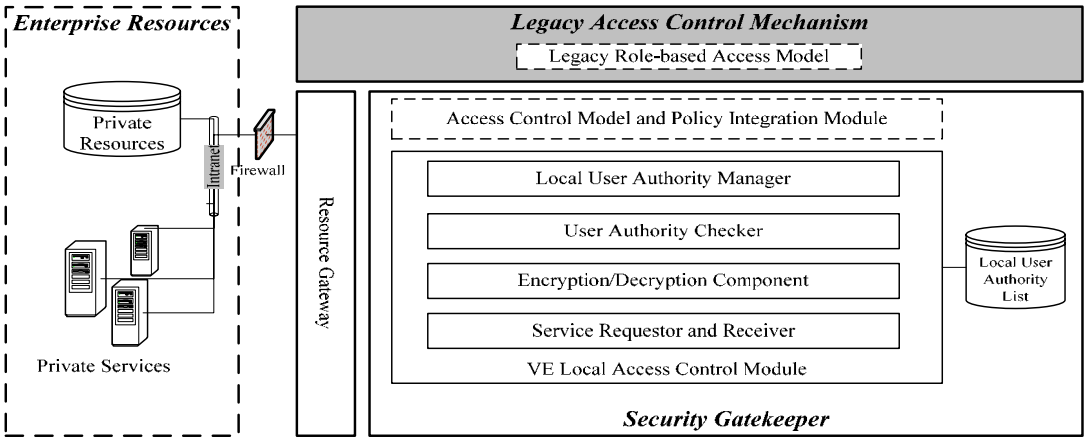


Fig. 8 Functional framework of security gatekeeper

- *Global Certificate Authority Center* (GCAC): Every user or enterprise must have a digital certificate to authenticate them within the Network. The GCAC, a third party, is responsible for certificate authentication and notifying VEACC of the results.

5.2 Certificate authentication, authority and access control approaches

In virtual enterprise access control, authenticating a user is an essential step before authorizing the user for any protected operation. Since VE members often change, the VE user authority has to be frequently updated to protect its resources. Therefore, the certificate, authorization and access control management are important in a VE. This section shows the operations related to this job. Analyzing the resource access requirement in virtual enterprise, regardless of public or private resources, in which they include two access modes to need integration and not integration. In addition to the access modes, peer-to-peer private resource access mode is often used, too. The following sub-sections will illustrate the approaches in order.

5.2.1 Approach for updating user authority list

When a user enters the VEAC system, the system must generate a user authority list, and update each SG's local user authority list and the VEACC's global user authority list. This approach is shown in Fig. 9 and explained as follows:

(1) User logs onto the VEACC and enters his personal data including name, validity period, public key information and a signed hash of the certificate data.
(2) VEACC authenticates the user's personal basic data; if the user data are incorrect, then the VEACC rejects the user.
(3) If the user data are correct, then the VEACC sends the user personal data to the GCAC to authenticate the digital certificate.
(4) GCAC sends the verification results to VEACC.
(5) If the user's digital certificate is correct, then the VEACC generates the user authorities and adds them to the global user authority list.
(6) VEACC decomposes the user authorities according to the enterprise owning each resource, and generates a local user authority list for each enterprise.
(7) VEACC sends a local user authority list of each enterprise to their SG.
(8) Each SG updates its local user authority list.
(9) SG informs VEACC that SG has completed the updating procedure.
(10) VEACC informs the user that he may access VE resources.

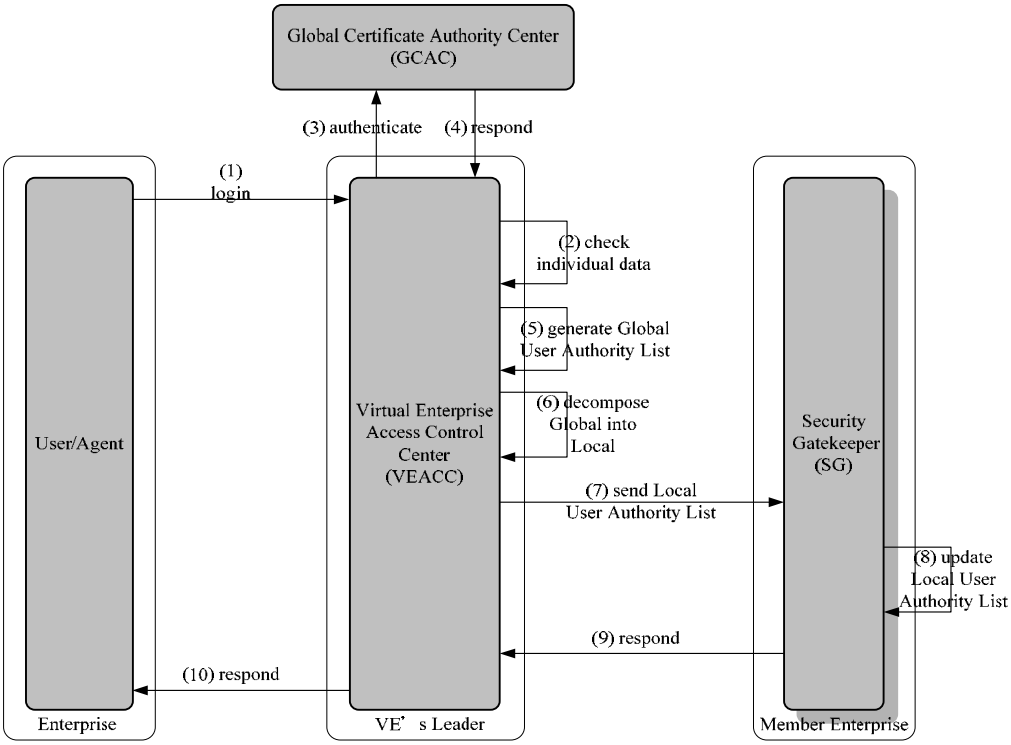


Fig. 9 Approach for updating user authority list

5.2.2 Approaches for accessing public resources

A variety of public resources in virtual enterprise is shared, some of which could need to be integrated. VEACC provides two approaches for accessing public resources with and without information integration, shown in Figs. 10 and 11, respectively. The information integration mechanism (IIM) supports the information format transformation among enterprises.

- **Approach for accessing public resources without information integration**

The approach for public resource access without information integration is shown in Fig. 10 and explained as follows:

(1) User/Agent in enterprise B requests access to Public Resources.
(2) VEACC receives the request, and searches the user authority from the Global User Authority List.
(3) If User's requested operation is allowed, then VEACC sends a call statement to Public Resources in a virtual enterprise platform.
(4) The Public Resources perform the service requested by User.
(5) The Public Resources directly respond with the results using an appropriate format to represent the User information.

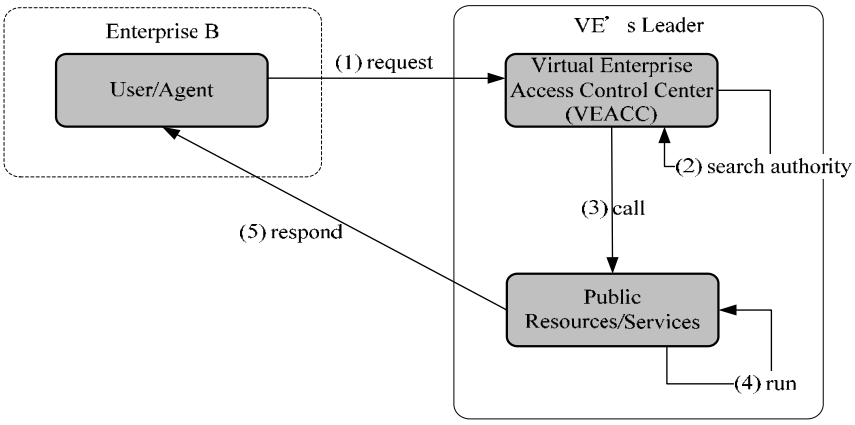


Fig. 10 Approach for public resource access without information integration

- **Approach for accessing public resources with information integration**

The approach for public resource access with information integration is shown in Fig. 11 and explained as follows:

(1) User/Agent in enterprise B requests access to Public Resources which need to be transformed into another format.
(2) VEACC receives the request, and searches the user authority from the Global User Authority List.
(3) If User's requested operation is allowed, then VEACC sends a call statement to Public Resources in a virtual enterprise platform.
(4) The Public Resources perform the service requested by User.
(5) The Public Resources directly respond with the results to Information Integration Mechanism (IIM).
(6) The IIM proceeds with information integration and transformation according to the information requirement of enterprise B.
(7) The IIM respond with the results using enterprise B's format to represent the responded information.

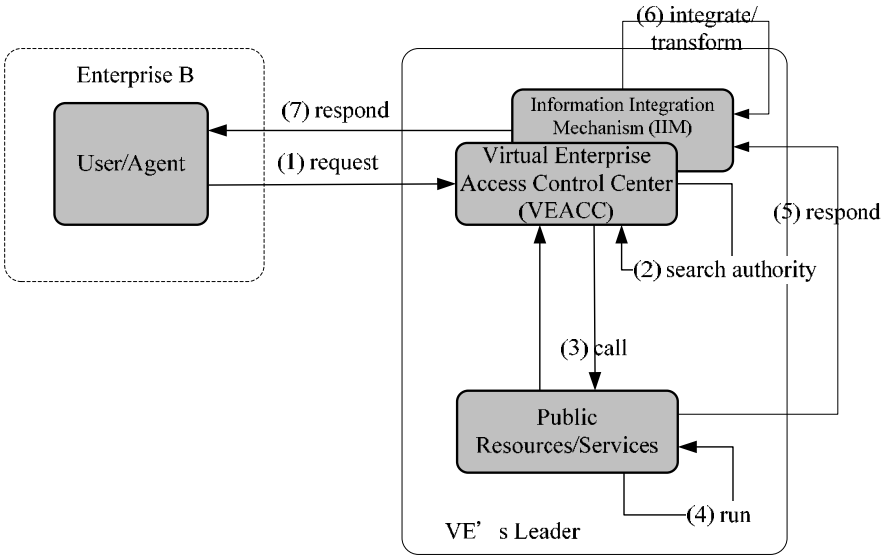


Fig. 11 Approach for public resource access with information integration

5.2.3 Approaches for accessing private resources

A variety of private resources in enterprise is shared, which could need integration or not. VEACC provides two approaches for accessing private resources with and without information integration, shown in Figs. 12 and 13, respectively.

- **Approach for accessing private resources without information integration**

The approach for accessing private resource without information integration is shown in Fig. 12 and explained as follows:

(1) User/Agent in enterprise B requests access to Private Resources.
(2) VEACC receives the request, and searches the user authority in the Global User Authority List. If the User is allowed to access the Private Resource, then the VEACC generates a pair of session keys.
(3.1) VEACC responds with one session key.
(3.2) Simultaneously, the VEACC sends to the SG the other session key and the User/Agent's request.
(4) SG verifies again the authority for the request.
(5) If the request is valid, then SG with gateway calls the requested Private Resource.
(6) The Private Resource in member enterprise A performs the service requested by User in enterprise B.
(7) The Resource/Service directly responds with the results using an appropriate information format and encrypting it using the session key.

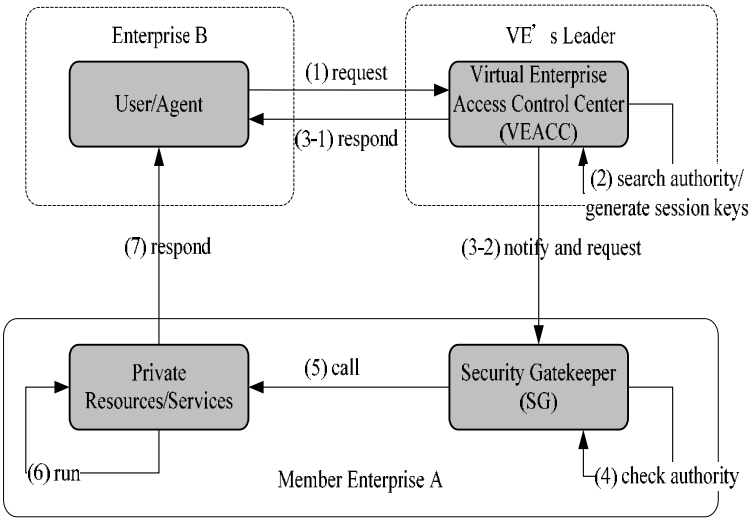


Fig. 12 Approach for private resource access without information integration

- **Approach for accessing private resources with information integration**

The approach for accessing private resource with information integration is shown in Fig. 13 and explained as follows:

(1) User/Agent in enterprise B requests access to Private Resources which need information integration and transformation.

(2) VEACC receives the request, and searches the user authority in the Global User Authority List. If the User is allowed to access the Private Resource, then the VEACC generates a pair of session keys.

(3-1) VEACC responds with one session key.

(3-2) Simultaneously, the VEACC sends to the SG the other session key and the User/Agent's request.

(4) SG verifies again the authority for the request.

(5) If the request is valid, then SG with gateway calls the requested Private Resource.

(6) The Private Resource in member enterprise A performs the service requested by User in enterprise B.

(7) The Resource/Service directly responds with the results using a standard information format to SG.

(8) The SG encrypts the results by using the session key and sends it to IIM.

(9) The IIM proceeds with information integration and transformation according to the information requirement of enterprise B.

(10) The IIM responds the results of request to User in enterprise B.

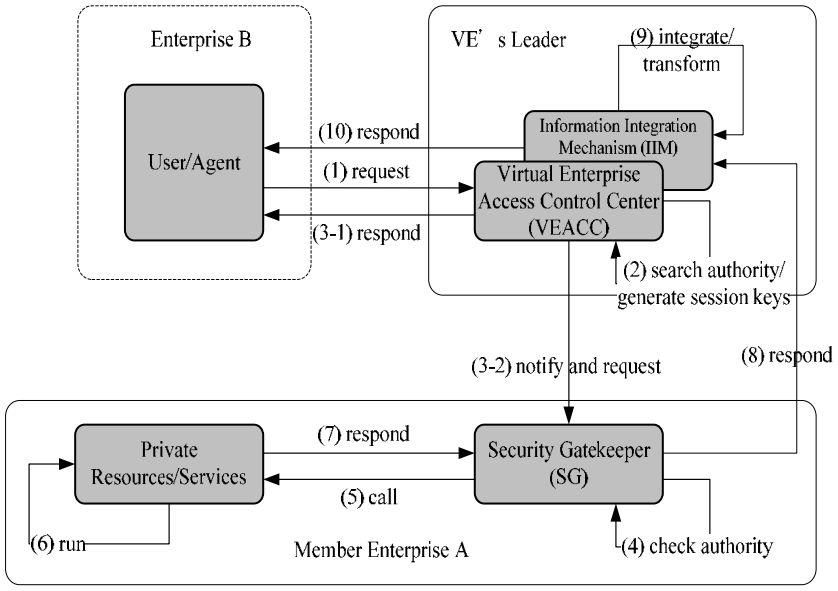


Fig. 13 Approach for private resource access with information integration

5.2.4 Approaches for accessing peer-to-peer private resources without information integration

In virtual enterprise environment, in order to speed up the efficiency of information access, the approach for accessing peer-to-peer private resources which need not to integrate is shown in Fig. 14, in which each step is introduced as follows.

(1) User logs onto the VEACC for requesting a credential and further enters his personal data including name, validity period, public key information and a signed hash of the certificate data.
(2) VEACC authenticates the user's personal basic data; if the user data are incorrect, then the VEACC rejects the user. If the user data are correct, then the VEACC sends the user personal data to the GCAC to authenticate the digital certificate.
(3) GCAC sends the verification results to VEACC.
(4) VEACC generates a credential for the user if the digital certificate is correct.
(5) VEACC responds the credential to the user.
(6) User sends the credential and request to SG.
(7) SG checks the credential and user authority.
(8) If the credential and user authority are legal, SG calls the private resource to supply service for the request.
(9) The private resource runs the request.
(10) The private resource responds the result to user.

In the approach, the steps (7), (8), (9) and (10) can be repeated to request other services during a timestamp.

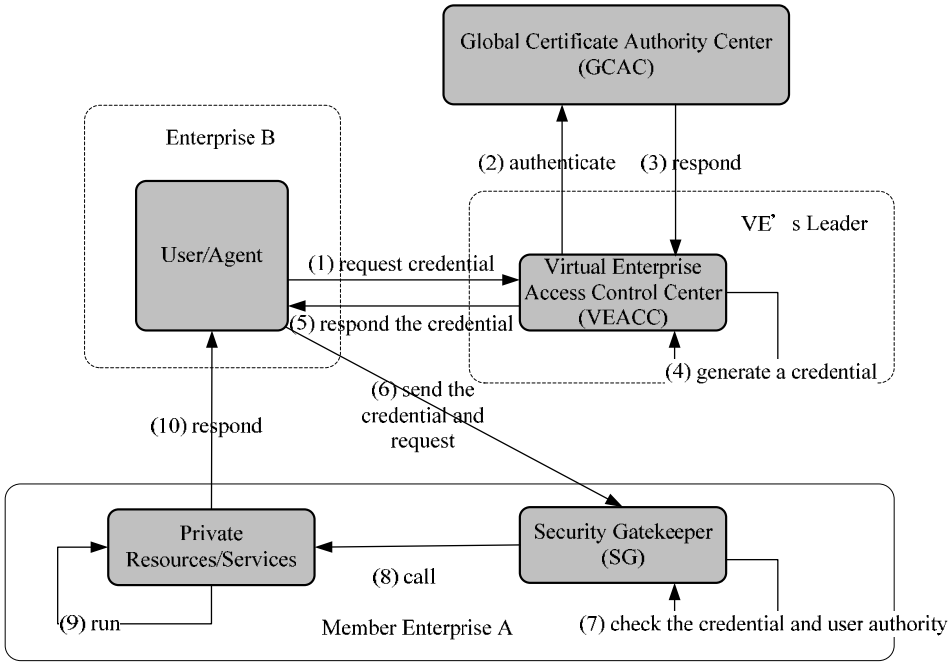


Fig. 14 Approach for accessing peer-to-peer private resources without information integration

6. Discussion and Conclusions

The aims of this study may help VEs to successfully solve the challenges of resource management and sharing among enterprises. The study has already accomplished the phase objective to propose a VEAC model, design the architecture of a prototype system and the functional frameworks of its core mechanisms, and develop the approaches for authentication and authorization in VE. However, the study has some deficiencies. For example, the non-RBAC model and integration of its access policies was not investigated. If an enterprise adopts non-RBAC models and other access policies, it must perform additional model-transferring process to transform them to RBAC in order to integrate them with VEAC project-based access control model.

6.1 Results and Contributions

The results and contributions of this study were as follows:

- The model may: (1) enables resources management and sharing in VE; (2) facilitate dynamic change of access right based on the organization structure of a VE; (3) preserve the access rights of users who are not affected under the change the organization of a VE or its members; (4) prevents to disclose business confidential information in virtual enterprising, and (5) ban all users working in an enterprise and its partners from accessing resources in the VE, when the enterprise drops out from the VE.
- The system architecture and approaches enable: (1) users from anywhere can take up to date information; (2) single authentication can entry multi-domains to access resources; (3) authorization considers not only individual privilege but also privilege from other workers that work together with him, and (4) the extent of resources sharing among workers depends on the cooperation relations among them and task requirements.

6.2 Further research

In the electronic commercial environment, resource management and sharing will become more complicated in the future. The proposed VEAC model solves access control and VE resource sharing problems. The implementation of the VEAC model-based access control system prototype is a great software engineering. In the future we will make up a distributed software engineering team to develop the system prototype using object-oriented software development methodology. However, some problems still need to be resolved.

(1) This study did not consider that the user might share a resource with unauthorized users, for example by copying it, after legally acquiring the resource.
(2) Algorithms based on the VEAC model should be developed to generate user authority.
(3) Methods for the access control server to call and use resources in the heterogeneous platform were not considered.
(4) An enterprise may adopt a non-RBAC-based scheme. Therefore, integrating different access control schemes or policies should be a focus points for future studies.
(5) Ideally, an enterprise should keep its original access control model when joining a VE. Therefore, a 'plug-and-play' access control integrating mechanism with a ability should be developed.
(6) An enterprise may participate in several competing VEs. Preventing the leaking of key technology or data should be considered.
(7) Future studies should adopt the XACML (eXtensible Access Control Markup Language) proposed by OASIS to develop access control policy frameworks enabling access strategies to be integrated among enterprises.

Acknowledgment

This research is financially supported by National Science Council of the Republic of China under Contract Nos: NSC94-2524-S-024-002, NSC94-2524-S-006-005 and NSC94-2524-S-006-006.

NSC94-2525-S-343-001

References

[1] A. Frenkel, H. Afsarmanesh, C. Garita, L.O. Hertzberger, Supporting Information Access Rights and Visibility Levels in Virtual Enterprise, Second IFIP working Conference on Infrastructures for Virtual Organizations: Managing Cooperation in Virtual Organizations and Electronic Business towards Smart Organizations, 2000.

[2] N. Mezzetti, Towards A Model for Trust Relationships in Virtual Enterprises,

Database and Expert Systems Applications, 14th International Workshop, 2003, pp. 420 - 424.

[3] T.J. Smith, L. Ramakrishnan, Joint Policy Management and Auditing in Virtual Organizations, Grid Computing, Fourth International Workshop, 2003, pp. 117 - 124.

[4] Y.M. Chen, M.W. Liang, Design and Implementation of a Collaborative Engineering Information System for Allied Concurrent Engineering, Int. J. of Computer Integrated Manufacturing, Vol. 13, no. 1, 1999, pp. 11-30.

[5] S. Oh, S. Park, Task-role-based Access Control Model, Information System, 2003, pp. 533-562.

[6] G.J. Ahn, Specification and Classification of Role-based Authorization Policies, Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003, pp. 202 - 207.

[7] R.A. Botha, J.H.P. Eloff, Designing Role Hierarchies for Access Control in Workflow Systems, 25th Annual International Computer Software and Applications Conference, 2001, pp. 117 - 122.

[8] C. Yang, C.N. Zhang, Designing Secure E-commerce with Role-based Access Control, IEEE International Conference on E-Commerce, 2003, pp. 313 - 319.

[9] F. Dridi, B. Muschall, G. Pernul, Administration of an RBAC System, Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004, pp. 187 - 192.

[10] A. Kern, A. Schaad, J. Moffett, Enterprise Role Administration: An Administration Concept for the Enterprise Role-based Access Control Model, Proceedings of the eighth ACM symposium on Access control models and technologies, 2003, pp. 33-40.

[11] C.J. Moon, D.H. Park, S.J. Park, D.K. Baik, Symmetric RBAC Model that Takes the Separation of Duty and Role Hierarchies into Consideration, Computers & Security, 2004, pp. 126-136.

[12] D. Shin, G.J. Ahn, J.S. Park, An Application of Directory Service Markup Language (DSML) for Role-based Access Control (RBAC), 26th Annual International Computer Software and Applications Conference, 2002, pp. 934 - 939.

[13] E.C. Cheng, An Object-oriented Organizational Model to Support Dynamic Role-based Access Control in Electronic Commerce Applications, Proceedings of the 32nd Annual Hawaii International Conference on System Sciences, Vol.: Track8 (1999), pages: 9.

[14] F.T. Alotaiby, J.X. Chen, A Model for Team-based Access Control (TMAC 2004),

International Conference on Information Technology: Coding and Computing, Vol. 1, 2004, pp. 450-454.

[15] J.S. Park, K.P. Costello, T.M. Neven, J.A. Diosomito, Access Management for Distributed Systems: A Composite RBAC approach for Large, Complex Organizations, Proceedings of the ninth ACM symposium on Access control models and technologies, 2004.

[16] E. Cohen, T.K. Roshan, W. Winsborough, D. Shands, Models for Coalition-based Access Control (CBAC), Symposium on Access Control Models and Technologies, 2002, pp. 97-106.

[17] L. Zhang, G.J. Ahn, B.T. Chu, A Rule-based Framework for Role-based Delegation and Revocation, ACM Transactions on Information and System Security (TISSEC), vol. 6, issue 3, 2003.

[18] M.H. Kang, J.S. Park, J.N. Froscher, Access Control Mechanisms for Inter-organizational Workflow, Proceedings of the sixth ACM symposium on Access control models and technologies, 2001.

[19] R. Nabhen, E. Jamhour, C. Maziero, RBPIM: a PCIM-based Framework for RBAC, Local Computer Networks, 28th Annual IEEE International Conference, 2003, pp. 52 - 61.

[20] G. Denker, J. Millen, Y. Miyake, Cross-domain Access Control via PKI, Third International Workshop on Policies for Distributed Systems and Networks, 2002, pp. 202 - 205.

[21] S. Osborn, Integrating Role Graphs: A Tool for Security Integration, Data & Knowledge Engineering, 2002, pp. 317-333.

[22] W. Yamazaki, H. Nishiyama, F. Mizoguchi, Design of Collaborative Agent System with Access Control for Smart-office Environment, Tenth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2001, pp. 205 - 210.

[23] C. Yang, C.N. Zhang, Secure Web-based Applications with XML and RBAC, Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, 2003, pp. 276 - 281.

[24] M. Coetzee, J.H.P. Eloff, Virtual Enterprise Access Control Requirements, Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on enablement through technology, 2003, pp. 285-294.

[25] D.F. Ferraiolo, R. Chandramouli, G.J. Ahn, S. I. Gavrila, Enterprise Role Administration: The role control center: features and case studies, Proceedings of the eighth ACM symposium on Access control models and technologies, 2003, pp. 12-20.

[26] G. Kolaczek, Specification and Verification of Constraints in Role Based Access Control for Enterprise Security System, Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003, pp. 236-240.

[27] H. Zhu, Some Issues of Role-based Collaboration, Canadian Conference on Electrical and Computer Engineering, vol. 2, 2003, pp. 687 - 690.

[28] J. Luo, D. He, Research on Object-oriented Role-based Access Control Model, Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003, pp. 132 - 135.

[29] J.D. Moffett, Control Principles and Role Hierarchies, Proceedings of the third ACM workshop on Role-based access control, 1998, pp. 63-69.

[30] K. Furst, T. Schmidt, G. Wippel, Managing Access in Extended Enterprise Networks, Internet Computing, IEEE, Vol. 6, issue 5, 2002, pp. 67 - 74.

Biographies

Mr. Tsung-Yi Chen is a Ph.D. candidate of Institute of Manufacturing Engineering, National Cheng Kung University, Taiwan, ROC and a Lecturer of Electronic Commerce Management Department, Nan Hua University in Taiwan, ROC. He gained his M.S. degree from Institute of Manufacturing Engineering, National Cheng Kung University, Taiwan, ROC in 2001 and the B.S. degree from Department of Applied Mathematics, Providence University, Taiwan, ROC in 1996. His research interests include Virtual Enterprise, E-Commerce and E-Business, Enterprise and Information Integration, and Access Control.

Dr. Yuh-Min Chen is currently a Professor and the Director of Institute of Manufacturing Engineering, National Cheng Kung University, Taiwan, ROC. He graduated from the Ohio State University with a Ph.D. degree in Industrial and Systems Engineering in 1991 and received his MS and BS degrees from National Tsing Hua University, Taiwan, ROC in 1981 and 1983 respectively. Before joining the faculty

of Institute of Manufacturing Engineering in 1994, he worked as a research engineer in Structural Dynamics Research Corporation, USA for three years. His current research interests include Enterprise Integration, Engineering Data and Knowledge Management, Computer-Aided Concurrent Engineering and Manufacturing Information Systems.

Dr. Hui-Chuan Chu is an Associate Professor of Department of Special Education, National University of Tainan in Taiwan, ROC. She received her Ph.D. degree from Columbia University in 1998. Her research interests are Knowledge Management, Teacher Knowledge, and Integration of Information Technology in Teacher Education.

Dr. Chin-Bin Wang is currently a Professor and the Chairman of Electronic Commerce Management Department, Nan Hua University in Taiwan, ROC. He received his Ph.D. degree in Computer Science from the City University of New York in 1995, and gained his MS degree from University of Southern California and BS degrees from National Tsing Hua University, Taiwan, ROC in 1985 and 1981 respectively. His research interests include Data Mining, Network Management, Engineering Data and Knowledge Management, System Integration.

附件(八)

Secure Resource Sharing on Cross-organization Collaboration Using a Novel Trust Method

Tsung-Yi Chen[1,2], *Yuh-Min Chen[1], Chin-Bin Wang[2], Hui-Chuan Chu[3], Huimei Yang[4]

[1]Institute of Manufacturing Engineering
National Cheng Kung University
Tainan, Taiwan
[2]Electronic Comerence Management Department
Nan Hua University
Chia-Yi, Taiwan
[3]National University of Tainan
Tainan, Taiwan
[4]Department of Business Administration
Tatung Institute of Commerce and Technology
Chia-Yi, Taiwan, ROC

*Corresponding author's e-mail: ymchen@mail.ncku.edu.tw
TEL: 886-6-2757575 ext. 63922
FAX: 886-6-2085334

Abstract

A virtual enterprise (VE) consists of a network of independent, geographically dispersed administrative business domains that collaborate with each other by sharing business processes and resources across enterprises to provide a value-added service to customers. Therefore, the success of a VE relies on full information transparency and appropriate resource sharing, making security and trust among subjects significant issues. Trust evaluation to ensure information security is most complicated in a VE involving cross-organization collaboration. This study presents a Virtual Enterprise Access Control (VEAC) Model to enable resource sharing for collaborative operations in the VE. A scenario for authentication and authorization in life cycle of a VE is then described to identify the main activities for controlling access. Also developed herein is a trust evaluation method based on the VEAC model to improve its security while safeguarding sensitive resources to support collaborative activities. The trust evaluation method involves two trust evaluation sub-models, one to evaluate the level of trust between two virtual enterprise roles, and another to measure the level of trust between two projects. The two sub-models support each other to make resource-sharing decisions, and are developed based on the concepts of direct, indirect and negative trust factors. Finally, an example of measuring the trust between two subjects is demonstrated after

introducing the two sub-models. The VEAC-based trust evaluation method enables the following: (1) secure resource sharing across projects and enterprises; (2) collaborative operation among participating workers; (3) increased information transparency, and (4) lowered information delay in VEs.

Keywords: Virtual enterprise, Resource sharing, RBAC, Trust, Access control, Collaboration.

1. Introduction

Most enterprises adopt a virtual enterprise business model for activities related to products and services required by customers. Virtual enterprises (VE) evoke notions of cooperation, cohesiveness and trust among coworkers from different organizations to accomplish common goals. Hence, VEs have to respond quickly to customer expectations by integrating processes, activities and resources from different enterprises through enterprise alliances [1]. In practice, a VE is implemented with a distributed and collaborative business process, in which individuals from different enterprises cooperate on business-related activities or processes by remote coordination, communication and control [2, 3, 4].

Effective virtual enterprising requires fully transparent and effective sharing of resources, including information, application systems and knowledge, throughout the business cycle [1]. Information sharing, including real-time capability, enables operational improvements and reduces the overall cost [5]. Information resources to support the practical operations in VE can be classified into three categories: (1) information brought by participating enterprises; (2) information generated by activities in a virtual enterprise, and (3) the information assets of a virtual enterprise. The three categoeies of information should be securely managed and shared with an appropriate mechanism. Charles *et al*. explored a dynamic coalition problem by emphasizing information sharing and security risks among groups [6]. Zha and Ding analyzed the necessity and impact of sharing information among supply chain partners in several sharing modes [7]. However, resource sharing introduces trust and authority management issues, and shows the significance of resource access comtrol.

Access control and sharing determines whether a subject can access resources controlled by another subject, and protects the confidentiality, integrity and availability of resources [8]. The subject, which is a member of the VE, can be an employee, role, agent or software application. Access control for VEs is difficult to accomplish because: (1) members of the VE frequently change; (2) VEs have many members with often complex inter-relationships; (3) VEs may be integrated or distributed, and (4) VEs are Internet-based and heterogeneous [9]. Because of the decentralized and dynamic characteristics in VE environments, access control for VE is impossible with traditional access control approaches [10, 11].

Trust management in an organization refers to complex relationships among individuals,

systems and organizational information management policies, and becomes particularly cumbersome in a VE, which involves cross-organizational activities [12]. Trust evaluation in a VE concerns safety and availability among individuals when delegating to partially trusted coworkers performing tasks concerning the aim of the VE. Therefore, the current trust model is not well suited to VEs due to its dynamic cooperative and collaborative properties. Trust management has been supported in part by some recent literature. Shand *et al.* in [13] presented a trust and risk framework to enable secure collaboration in ubiquitous and pervasive computer systems. Tran *et al.* in [14] developed a trust-based peer-to-peer access control framework with a scoring system to assess the access value by combining direct and indirect trusts with direct and indirect contributions. Dimmock *et al.* applied the OASIS access control system, and extended role-based policy language to make decisions based on trust and risk analysis [15]. Barrett and Konsynski proposed a method for classifying inter-organization information sharing systems [16]. Zuo and Panda developed a labeling scheme after analyzing the issue of trust from two perspectives, the 'subject' and 'object' [17]. Although access control across multi-enterprises has rarely been studied, a trust evaluation method should be developed for a VE for four reasons: (1) a VE differs from a peer-to-peer environment; (2) no model enables control of resource sharing across organization boundaries to support collaborative and cooperative business activities; (3) no model considers the trust evaluation among coworkers and projects [18], and (4) the resources accessed by users in the VE cannot be predicted.

This study adopts the VEAC model to improve resource sharing and information transparency among enterprise members, and the VEAC-based trust evaluation method to increase the security, flexibility and scalability of resource sharing. One difficulty in measuring the trust of a subject among virtual enterprises is the lack of a method to examine the degree to which a subject should be trusted [17]. This study first introduces a Virtual Enterprise Access Control (VEAC) model for collaborative operation among each participating enterprise [19]. Second, a scenario for authentication and authorization in virtual enterprise is presented to find the main authentication and authorization activities, and to indicate the interactive relationships among core access control mechanisms. Finally, a trust evaluation method based on the proposed VEAC model is developed by analyzing security problems, role rights, qualifications & responsibilities, project relations, cooperative relations and role hierarchical relations, which are the core components of VEAC. The VEAC-based trust method allows: (1) resource sharing across projects and enterprise boundaries; (2) secure collaborative operation among participating coworkers; (3) increased information transparency, and (4) reduced information delays in a VE.

2. Virtual enterprise access control model

Although Wang *et al.* presented a Virtual Enterprise Access Control (VEAC) Model in [19], that study did not describe it in detail. Therefore, this section introduces the VEAC Model and its

basic components as depicted in Fig. 1. The model is derived from the resource management requirements and the characteristics of a VE, and includes two sub-models, a project-based access control (PBAC) model for managing public resources stored in a VE, and a role-based access control (RBAC) model for handling private resources held on individual enterprise members.

(Insert Fig. 1 Virtual Enterprise Access Control (VEAC) Model)

2.1 Role-based Access Control Model

RBAC involves three fundamental components, the base model, role hierarchy and constraints. The bottom of Fig. 1 shows the RBAC Model [20-23]. Elements and relationships in RBAC are described simply as follows:

- User (U), also called Subject, denotes a human, web service, application or agent in an enterprise.
- Role (R) denotes a set of functional jobs or responsibilities, and is expressed as a set of permissions.
- Private Object (PrivateO) is a sub-class of Object class, and denotes resources in an enterprise associated with private permissions.
- Private Permission (PrivateP) is the approval of a particular mode of access to one or more private objects.
- Session (S) represents each session, through which users map to one or more roles.

The RBAC model assigns each user to play roles associated with private permissions given to perform operations on a private object. A user only plays a role at a session where he can activate a subset of Roles assigned to it. The following three relations among Roles denote the privilege assignment of role: *Role Hierarchy*, *Static Separation of Duty* (SSD), and *Dynamic Separation of Duty* (DSD). The RBAC model utilizes two relationships to represent the aggregation relationships between two elements: EM-R-A between the Enterprise Member and Role elements, representing the Role elements in each Enterprise element, and EM-U-A between the Enterprise Member and User elements, representing the User elements belonging to the Enterprise Member element.

2.2 Project-based access control model

The PBAC model is shown in the upper layer of Fig. 1. The core concept of model development, elements and relations in the PBAC model are introduced and defined in the following sub-sections.

2.2.1 Fundamental elements

This sub-section introduces the fundamental elements of the PBAC model in the Set theorem:

- *Virtual Enterprise* (VE) = {*ve*: *ve* is a dynamic Internet organization which consists of enterprise members (EM) performing a project to achieve one common business goal.}
- *Enterprise Member* (EM) = {*em*: *em* can be a substantive enterprise organization, VE or individual, and is a VE member, with at least one worker participating directly in the VE activities.}
- *Non-Enterprise Member* (NEM) = {*nem*: *nem* can be a substantive enterprise organization, VE or individual, but not a VE member. A nem has at least one worker participating directly in activities of enterprise members, and the activities have direct relations with functional tasks of VE.}
- *Project* (P) = {p: p is the set of functional tasks, projects and sub-projects, which is performed by a VE.}
- *Functional Task* (FT) = {*ft*: *ft* is a set of VE activities, which has a common objective and is performed by several virtual enterprise roles (VER).} A functional task involves five attributes:
  (1) *FT-state* records the state of the functional task being performed;
  (2) *FT-stage* records current timestamp of a functional task for appropriate resource sharing according to its states;
  (3) *Allowed-reference* is a Boolean data type to decide whether the functional task can be referred by relative functional task in a post-version project;
  (4) *Allowed-sub-project* decides whether the functional task can be referred by its sub-projects; and
  (5) *Allowed-main-project* decides whether the functional task can be referred by its super-project.
- *Virtual Enterprise Role* (VER) = {*ver*: *ver* is a virtual role created to enable professional division within VE, which is assigned to perform more than one functional task (FT).}
- *Object* (O) = {*o*: *o* is an information resource including public and private resources which can be database, entity, attribute, tuple, document, XML document, application, software component or knowledge.}
- *Public Object* (PublicO) = {*public-o*: *public-o* is a subset of objects, which is owned by a VE and stored in a VE's common repository.}
- *Operation* = {*op*: *op* is a set of access authorities, such as "write", "read" and "execute".}
- *Public Permission* (PublicP) = {*public-p*: *public-p* is a permitted mode of access to a public object.}
- *Permission* = {*x*: $x \in PublicP \cup PrivateP$.}
- *Project Access Control Policy* (PACP): PACP identifies which project resources are protected and shared according to the relations among projects and the sharing rules, and what activities are forbidden in the virtual enterprise scope.

2.2.2 Foundational assignments

The various assignment relations among elements are defined as follows:

- *FT-S-PublicP-A*: a triple assignment among three elements: *Functional Task*, *Stage*, and *Pubic Permission*. It is represented by $R_{ft\text{-}s\text{-}publicp\text{-}a}$={(*ft*, *st*, *public-p*): $ft \in FT$, $st \in Stage$, and $public\text{-}p \in PublicP$,} means that public permission *public-p* is assigned to functional task *ft* in stage *s*.
- *P-VER-A*: a one-to-many binary assignment is represented by $R_{p\text{-}ver\text{-}a}$={(*p*, *ver*): $p \in P$, $ver \in VER$,

and p "involves" ver}.

- *VER-FT-A*: a many-to-many binary assignment is represented by $R_{ver\text{-}ft\text{-}a}$={($ver$, ft): $ver \in VER$, $ft \in FT$, and ver "performs" ft}.
- *VE-EM-A*: a many-to-many binary assignment is represented by $R_{ve\text{-}em\text{-}a}$={($ve$, em): $ve \in VE$, $em \in EM$, and em "is a members of" ve}.
- *VE-P-A*: a one-to-many binary assignment is represented by $R_{ve\text{-}p\text{-}a}$={(ve, p): $ve \in VE$, $p \in P$, and ve "performs" p}.
- *EM-NEM-A*: a many-to-many binary assignment is represented by $R_{em\text{-}nem\text{-}a}$={($em$, nem): $em \in EM$, $nem \in NEM$, and nem "supports" em "to perform some tasks of the" *VE-EM-A_virtual_enterprise*(em)}.
- *Functional Task Workflow* (FTWf): a many-to-many binary assignment is represented by R_{FTWf}={(ft_i, ft_j): ft_i, $ft_j \in FT$, p_i, $p_j \in P$, $ft_i \subset p_i$, $ft_j \subset p_j$, $i \neq j$, ft_i is a event-functional task of the action-functional task ft_j} means ft_j is authorized to use the public permissions of ft_i while ft_i is accomplished.
- *Correspondence*: a one-to-one binary relation on FT is represented by $R_{correspondence}$={(ft_i, ft_j): ft_i, $ft_j \in FT$, p_i, $p_j \in P$, $ft_i \subset p_i$, $ft_j \subset p_j$, $i \neq j$, ft_i "is the pre-version of" ft_j while ft_j is the post-version of" ft_i}.
- *EM-U-A*: a one-to-many binary assignment is represented by $R_{em\text{-}u\text{-}a}$={(em, u): $em \in EM$, $u \in U$, and em "have an employee" u}.
- *NEM-U-A*: a one-to-many binary assignment is represented by $R_{nem\text{-}u\text{-}a}$={($nem$, u): $nem \in NEM$, $u \in U$, and nem "have a employee" u}.
- *R-VER-A*: a many-to-many binary assignment is represented by $R_{r\text{-}ver\text{-}a}$={($r$, ver): $r \in R$, $ver \in VER$, and r "is assigned to play" ver}.
- *U-VER-A*: a many-to-many binary assignment is represented by $R_{u\text{-}ver\text{-}a}$={($u$, ver): $u \in U$, $ver \in VER$, and u "is assigned to play" ver}.

2.2.3 Project relations

A Project Relation (R_p) describes the interactions, cooperation modes and priority between two projects, and determines the level of resource sharing among them. Different project relations may exist between two projects, and project relations may change with time based on project management and sharing requirements. To introduce the project relations, given a set Project (P) and $x, y \in P$, a binary relation Project Relation (R_p) on P is a subset of $P \times P$. The project relation is split into five sub-relations:

- *Subset Relation* (R_{ps}) describes a project "main-project", which is decomposed into several projects "sub-projects" to be executed by different virtual enterprises. A main-project is permitted to access the resources of its sub-project, but an administrator may set or disable this capability. The subset relation is denoted by R_{ps}={(x, y): $x, y \in P$, $x \neq y$, and x "is a subset of" y}.

- *Version Relation* (R_{pv}) describes a project y called the "post-version project", which is extended from a project x called "pre-version project", and which is planned with reference to the pre-version project. Hence, the pre- and post-version projects have similar targets, functional tasks and participants. The version relation may result in correspondences between functional tasks of the two projects. The relation is represented by R_{pv}={(x, y): $x, y \in P$, $x \neq y$, and x "is the pre-version of" y}.

- *Reference Relation* (R_{pr}) describes a project x, called the "referring project", referring to the

resources in another project y, called the "referred project". If the reference relation exists between two projects, then users in the referring project can refer to the resources of the referred project. The functional task involved in the referred project is allowed to be referred as long as the value of its attribute "allowed-reference" is "true". The relation is given by $R_{pr}=\{(x, y)$: $x, y \in P, x \neq y$, x "refers to resources in" y, and $(\neg \exists xR_{pe}y) \wedge (\neg \exists yR_{pe}x)\}$.

- *Process Relation* (R_{pp}) indicates the execution sequence of two sub-projects, and determines the time for sharing project resources. When a project is split into several sub-projects, the process relation can be adopted to indicate the executive sequence of all sub-projects. While the relation is constructed on two projects, the administrator must specify the sequences of related functional tasks across project boundaries. The relation is represented by $R_{pp}=\{(x, y)$: $x, y, z \in P, x \neq y \neq z, (\exists xR_{ps}z) \wedge (\exists yR_{ps}z)$, and x "must be achieved, then start" $y\}$.

- *Exclusive Relation* (R_{pe}) denotes that two projects are mutual conflicting, indicating that the resources of the two projects cannot be referred to by each other. The relation is represented by $R_{pe}=\{(x, y)$: $x, y \in P, x \neq y$, x "conflicts with" y, and $(\neg \exists xR_{pr}y) \wedge (\neg \exists yR_{pr}x)\}$.

2.2.4 Cooperation modes between two VERs

This sub-section presents three cooperation modes among virtual enterprise roles according to the resource sharing requirements for collaborative operations in the VE.

Cooperation Mode (R_c) describes interactions among VERs based on the dependent level of their duties. Given a set Virtual Enterprise Role (VER), x and $y \in VER$, a binary relation Cooperation Relation (xR_cy) on VER is a subset of $VER \times VER$, which is differentiated into three cooperation relations. For convenience in the following discussion, two items are first defined in terms of authority inheritance. According to the cooperative mode, a virtual enterprise role may inherit strongly or weakly the privileges from the other virtual enterprise role. The *strong inheritance* indicates that the privileges of a VER can be completely inherited by the other VERs, while the *weak inheritance* means that the privileges can only be partially inherited, i.e. only some privileges of a VER are inhereited.

- *Dependent Single-task Mode* ($xR_{cds}y$) : The dependent single-task mode is a binary relation and represented by $R_{cds}=\{(x, y)$: $x, y \in VER, x \neq y, \exists (x, ft_1), (y, ft_1) \in VER\text{-}FT\text{-}A \rightarrow FT\text{-}PublicP\text{-}A\_public\_permission(\{VER\text{-}FT\text{-}A\_functional\_task(x)$: $(x, ft) \in VER\text{-}FT\text{-}A\})$ are inherited strongly by virtual enterprise role y, and $FT\text{-}PublicP\text{-}A\_public\_permission(\{VER\text{-}FT\text{-}A\_functional\_task(y)$: $(y, ft) \in VER\text{-}FT\text{-}A\})$ are inherited strongly by virtual enterprise role x, and $(\neg \exists xR_{cdm}y) \wedge (\neg \exists yR_{cdm}x) \wedge (\neg \exists xR_{ci}y) \wedge (\neg \exists yR_{ci}x)\}$ means that VER x and y cooperate to perform a functional task ft_1, and they have the same access privilege to all its resources.

- *Dependent Multi-task Mode* ($xR_{cdm}y$): The dependent multi-task mode is a binary relation and represented by $R_{cdm}=\{(x, y)$: $x, y \in VER, x \neq y, \forall (x, ft_x), (y, ft_y) \in VER\text{-}FT\text{-}A \rightarrow FT\text{-}PublicP\text{-}A\_public\_permission(\{VER\text{-}FT\text{-}A\_functional\_task(x)$: $(x, ft_x) \in VER\text{-}FT\text{-}A\})$ are inherited weakly by virtual enterprise role y, and

FT-PublicP-A_public_permission($\{$*VER-FT-A_functional_task*(y): (y, ft_y) $\in$ *VER-FT-A*$\}$) are inherited weakly by virtual enterprise role x, and $(\neg \exists xR_{cds}y) \wedge (\neg \exists yR_{cds}x) \wedge (\neg \exists xR_{ci}y) \wedge (\neg \exists yR_{ci}x)\}$ means that VER x and y perform related functional tasks separately and outputs of the functional tasks are referred to each other.

- *Independent Mode* ($xR_{ci}y$): The independent mode is a binary relation and represented by $R_{ci}=\{(x, y)$: $x, y \in VER, x \neq y$, *FT-PublicP-A_public_permission*($\{$*VER-FT-A_functional_task*(x): (x, ft_x) $\in$ *VER-FT-A*$\}$) are not inherited by virtual enterprise role y, and *FT-PublicP-A_public_permission*($\{$*VER-FT-A_functional_task*(y): (y, ft_y) $\in$ *VER-FT-A*$\}$) are not inherited by virtual enterprise role x, and $(\neg \exists xR_{cds}y) \wedge (\neg \exists yR_{cds}x) \wedge (\neg \exists xR_{cdm}y) \wedge (\neg \exists yR_{cdm}x)\}$ means that VER x and y perform independent functional tasks separately, disregarding their outputs. If two virtual enterprise roles work in an independent mode, they may not have each other's access privileges for functional tasks performed by them.

2.2.5 Properties of relations

To avoid security problems caused by privilege expansion resulting from element relations, and to strengthen private and public resource security, three binary relation properties — reflexive, symmetric, and transitive — are applied to the above relations. In a project formation stage, enterprise members in a VE determine whether each cooperation mode and project relation complies with these three properties. Each enterprise member can then identify these three properties based on its own resource sharing rules. The enterprise can also set the *depth* of the transitive property, and require symmetric and transitive properties to be valid only in the same *department*.

2.3 Role Relation Net (RRN)

Figure 2 shows a Role Relation Net (RRN), which is an applied example of the VEAC model. An RRN comprises the basic elements and relations defined in Section 2, which identify the interactive relations among projects, cooperation modes, roles and hierarchical relations in enterprise members, assignment relations between users and roles, and relations between roles and VE roles. In the RRN, through project relations to facilitate the resource sharing across projects, cooperation modes among VERs to enhance the information transparency of a VE, and roles and hierarchical relations to simplify assignment of privileges, users can be assigned proper privileges within a timeframe based on roles played by users and VERs used by roles. Section 4.3 illustrates the proposed trust evaluation method uisng the RRN as an example.

(Insert Fig. 2 Part of a Role Relation Net (RRN))

3. Scenario for authentication and authorization in virtual enterprise

The IT environments of large, distributed VEs generally consist of various platforms and applications. Subjects can access various resources deployed on different platforms. Two fundamental access control functions, authentication and authorization, and other related access control activities are shown as Fig. 3 and introduced below:

- Constructing the VEAC model: when a VE is organized, all enterprise members in the VE need to plan the VE objectives, processes, schedules and resources collaboratively. Administrators in this stage must construct the VEAC model, including the design of all elements and the assignments among elements, to enable resource sharing and reuse. Consequently, a VEAC specification is produced from the constructed VEAC model.

- Identifying the project access control policy: when a VE is formed, a project access control policy (PACP) should be identified based on the regulations of the VE for resource usage and sharing.

- Determining the resource threshold: the owner of each resource can set or change the resource threshold according to the secure requirement of dynamic business environment. Each resource involves both the VER and project thresholds, which are recorded in the resource list.

- Generating user authorization: when a user logs into the virtual enterprise access control system, the user authorization list is generated from private and public authorization algorithms which analyzes the PACP, VEAC specification and resource list. The trust evaluation method is then applied to assess the trust values for the VER and project. Based on these trust values, the system then prunes the user authorization list of trust values that are lower than the threshold of a resource. Finally, the pruned user authorization list is split into local user authorization lists, which are deployed on each enterprise member's access control mechanism.

- Controlling access: when a user successfully logs in, and the user authorization list is generated and deployed, the user can request access to the private resources stored in all enterprise members and the public resources stored in the virtual enterprise based on the user authorization list.

(Insert Fig. 3 Access control framework in a virtual enterprise)

4. Trust evaluation method

This section refines and redefines the concept of direct and indirect trusts presented in some other studies, and proposes the concept of a negative trust to improve the level of trust, thus enhancing the match among the requirements of practical virtual enterprise environments. The direct and indirect trust values are defined as the *positive interrelated coefficient*, which intensifies

the level of trust between two VERs, while the negative trust value is defined as the *negative interrelated coefficient*, which enables the sub-models to decrease the level of trust between two VERs. This section develops a trust evaluation method from the subject interaction perspective, which is based on the VEAC Model, and which expands the concept of direct and indirect trusts. The trust evaluation method is used to measure the level of belief or disbelief among two subjects (virtual enterprise role and project) for resolving the trust issues resulting from unclear assignment among elements and secure resource sharing across enterprise and project boundaries. This section describes various trust functions based on: (1) cooperation modes between two VERs or project relations between two projects; (2) dependence on responsibilities between two subjects; (3) the intersectional ratio of resources used in performing two functional tasks, and (4) the intersectional ratio of enterprise members participating in two projects. Figure 4 illustrates depicts the structure and significant features of the trust method containing two sub-models. The details are introduced as follows:

(1) *Trust evaluation sub-model for VER* is adopted to assess the trust level from one VER to another. The trust evaluation sub-model for a VER comprises a direct trust function, indirect trust functions at different depths and a negative trust function, as follows: (a) the *direct trust function* is calculated from the intersection ratio of the functional task assignments based on the cooperative mode between two VERs; (b) the *indirect trust functions* are determined from the direct trust function from one VER to another via the others (third-VERs), and (c) the *negative trust function* is obtained by considering the mutual relationships among the trustee, trusted and their third-VERs, based on the modes of cooperation among them.

(2) *Trust evaluation sub-model for projects* is employed to determine the trust level from the perspective of a particular project to another. Its value is obtained from various project relations and the resource assignment. The trust evaluation sub-model for a project also uses direct, indirect and negative trust functions to determine the trust value between two projects. The direct trust function of a project is calculated by combining the version, subset, reference and process direct trust values with an exclusive direct trust value. The concepts of development of the indirect and negative trust function for project resemble the indirect and negative trust functions of the trust sub-model of a VER.

(Insert Fig. 4 Structure of the trust evaluation method)

4.1 Trust evaluation sub-model for virtual enterprise role

This sub-section describes the trust evaluation sub-model for a virtual enterprise role, including a direct trust function, indirect trust functions at different depth, a negative trust function and a trust function.

4.1.1 Trust evaluation functions for virtual enterprise role

The part of a Role Relation Net (RRN) displayed in Fig.5 includes several VERs and cooperative modes linking VERs, denoting the direct and indirect trusts for a VER. As demonstrated in Fig. 5, the solid line between two VERs is the direct trust, and the dashed line between two VERs represents the indirect trust. The rules of cooperation between VERs allow only one direct trust between two VERs. However, the indirect trust value can exceed 1 when the transitive depth of the cooperation mode exceeds 1. The three trust classes are defined as follows:

(Insert Fig. 5 Part of Role Relation Net (RRN) denoting the direct and indirect trusts for VER)

- *Direct Trust* from ver_i to ver_j, $DT_{ver}(ver_i, ver_j)$, is defined as the level of trustworthiness of ver_j for ver_i, i.e., the level to which the trusted subject (ver_j) is believed by the trustee subject (ver_i). The two subjects (virtual enterprise roles) are regarded as nodes, and the cooperative mode linking a trusted subject with a trustee subject is treated as an edge with a trust degree. The risk of accessing an unauthorized resource via different cooperative modes between the trusted and trustee VERs might depend on the level of dependence upon the responsibilities assigned to the two VERs and their cooperation mode. Function 1 shows the direct trust function. Therefore, one of the three cooperative modes can be adopted to lead the trust value in the range [0, 1].

$$\mathrm{DT}_{\mathrm{ver}}\left(ver_i, ver_j\right) = \begin{cases} 1 & \text{if } \mathrm{R_c} = R_{cds} \\ |\mathrm{FT_i} \cap \mathrm{FT_j}| \,/\, \mathrm{Min}\{|\mathrm{FT_i}|, |\mathrm{FT_j}|\} & \text{if } \mathrm{R_c} = R_{cdm} \\ 0 & \text{if } \mathrm{R_c} = R_{ci} \end{cases} \quad (1)$$

Where

$DT_{ver}(ver_i,ver_j)$: direct trust of ver_j for ver_i;

ver_i: trustee VER;

ver_j: trusted VER;

R_c: cooperative mode including R_{cds}, R_{cdm} and R_{ci};

R_{cds}: dependent single-task cooperative mode;

R_{cdm}: dependent multi-task cooperative mode;

R_{ci}: independent cooperative mode;

FT_i and FT_j : the functional tasks performed by virtual enterprise role ver_i and ver_j,

respectively;

$|FT_i|$ and $|FT_j|$: numbers of functional tasks assigned to ver_i and ver_j, respectivey, and

$|FT_i \cap FT_j|$: number of functional tasks assigned simultaneously to both ver_i and ver_j.

- *Indirect Trust* from ver_i to ver_j, $IT_{ver}(ver_i, ver_j)$, is expressed as the level of trustworthiness of ver_j for ver_i via third-virtual enterprise roles (third-VERs) that interact with ver_i, ver_j or both, such as ver_1, ver_{l1} and ver_{l2} in Fig 5. The indirect trust can be considered as a path composed of edges connecting ver_i with ver_j via different third-VERs. Hence, the indirect trust can involve zero or more paths from a trustee subject to a trusted subject, where the number of the paths is determined from the number of the third-VERs that can cooperate directly with least one of the two subjects. The indirect trust function is derived from the direct trust function by considering all edges of a path from the trustee subject to the trusted subject. When the transitive property of the cooperation mode is available and its depth equals 2, the indirect trust function at depth 2 is defined as Function 2, which utilizes the product of two direct trust functions. The total number of multiple indirect trusts at depth 2 is then averaged to keep IT_{ver} in the range [0, 1].

$$\mathrm{IT}_{\mathrm{ver}_2}(ver_i, ver_j) = \sum_{l=1}^{k_2} \left[DT_{ver}(ver_i, verI_l) \times DT_{ver}(verI_l, ver_j) \right] \Big/ \mathrm{k}_2 \qquad (2)$$

Where

$\mathrm{IT}_{\mathrm{ver}_2}(ver_i, ver_j)$: indirect trust of ver_j for ver_i at depth 2;

$\mathrm{DT}_{\mathrm{ver}}(ver_i, ver_j)$: direct trust of ver_j for ver_i;

$verI_l$: third-virtual enterprise role (third-VER) that cooperates with ver_i and ver_j simultaneously, and

k_2: number of third-VERs that cooperate with ver_i and ver_j simultaneously, i.e., the number of paths from ver_i to ver_j via $\mathrm{ver}I_l$ while depth equals 2, $1 \le l \le \mathrm{k}_2$.

The indirect trust functions at depth 3 and beyond can be obtained from Function 2. The indirect trust function at depth 3 is represented in Function 3.

$$\mathrm{IT}_{\mathrm{ver}_3}(ver_i, ver_j) = \sum_{l=1}^{k_3} \left[DT_{ver}(ver_i, verI_{l1}) \times DT_{ver}(verI_{l1}, verI_{l2}) \times DT_{ver}(verI_{l2}, ver_j) \right] \Big/ \mathrm{k}_3 \qquad (3)$$

Where

$\mathrm{IT}_{\mathrm{ver}_3}(ver_i, ver_j)$: indirect trust of ver_j for ver_i at depth 3;

$verI_{l1}$: third virtual enterprise roles which directly cooperate with ver_i and $verI_{l2}$;

$verI_{l2}$: third virtual enterprise roles which directly cooperate with ver_j and $verI_{l1}$, and

k_3: number of paths from ver_i to ver_j at depth 3.

Finally, the indirect trust function is denoted in Function 4, which must be limited by Equation 5 in which the weighted factors for indirect trust at various depths are determined by the administrator, and the sum of the all weighted factors must equal 1.

$$\mathrm{IT}_{\mathrm{ver}}(ver_i, ver_j) = \sum_{w=2}^{\text{max-depth}} \alpha_w \times IT_{ver_w} \quad (4)$$

$$\sum_{w=2}^{\text{max-depth}} \alpha_w = 1 \quad (5)$$

Where

$IT_{ver}(ver_i,ver_j)$: total indirect trust value of ver_j for ver_i;

α_w: trust weighted factor for indirect trust value at depth w, $2 \leqq w \leqq$ max-depth; and

max-depth: maximal depth of available transitive property.

- *Negative Trust* from ver_i to ver_j, $NT_{ver}(ver_i, ver_j)$, is defined as the level of untrustworthiness of ver_j for ver_i, and is adopted to decrease the level of trust between ver_i and ver_j. Figure 6 shows the part of Role Relation Net (RRN) denoting the negative trust for the VER. The negative trust function defined in Function 6 rises when the trusted and trustee subjects cooperate with third-VERs using different cooperation modes. All third-VERs may be categorized into three groups. The numbers of the three third-VERs are represented by variables *k*, *n* and *p*, which are defined in Function 6. Consequently, the negative trust is in the range [0, 1].

(Insert Fig. 6 Part of Role Relation Net (RRN) representing the negative trust for VER)

$$\mathrm{NT}_{\mathrm{ver}}(ver_i, ver_j) = \sum_{m=1}^{n} DT_{ver}(ver_j, ver_{lm}) \Big/ (k + n - \mathrm{p}) \quad (6)$$

Where

$NT_{ver}(ver_i,ver_j)$: negative trust of ver_j for ver_i;

k: number of third-VERs cooperating with ver_i and ver_j simultaneously, i.e., the number of indirect trust values from ver_i to ver_j;

n: number of third-VERs that cooperate with ver_j with either cooperation modes R_{cds} or R_{cdm} and without ver_i;

p: number of third-VERs that cooperate with ver_j via the cooperation mode R_{ci} and without ver_i; and

ver_{lm}: third-VERs that cooperate with ver_j with either cooperation modes R_{cds} or R_{cdm} and without ver_i.

In contrast to variable *p* in Function 6, variables *k* and *n* enable the negative trust value to raise the trust level for the VER.

The trust function for VER as displayed in Function 7 is obtained by combining direct trust (DT_{ver}), indirect trust (IDT_{ver}) and negative trust (NT_{ver}), in which Eq. 8 should suffice irrespective

of how the weighted factors (C_{D1}, C_{I1} and C_{N1}) are set. The three weighted factors are determined by project administrators based on the influences of the direct, indirect and negative trusts on the trust evaluation sub-model for VER. Intuitively, if a trust value contributes more in terms of data value, it should be weighted more in the trust value calculation. Each resource in a virtual enterprise involves both a virtual enterprise role threshold and a project threshold (refer to Section 2) which can be frequently adjusted by the resource owner to adapt to the requirement of the virtual enterprise environment for resources sharing. When these three coefficients are altered, Function 7 can provide an adequate secure information sharing method. The trust value for VER (T_{ver}) is in the range [-1, 2] under the limitations of Eq. 8. The secure threshold of each resource is high when T_{ver} approaches 2, and is low when T_{ver} approaches -1.

$$T_{ver}(ver_i, ver_j) = C_{D1} DT_{ver}(ver_i, ver_j) + C_{I1} IT_{ver}(ver_i, ver_j) - C_{N1} NT_{ver}(ver_i, ver_j) \quad (7)$$

$$C_{D1}, C_{I1} \text{ and } C_{N1} = [o, 1] \quad (8)$$

Where

C_{D1}: trust weighted factor for the direct trust;

C_{I1}: trust weighted factor for the indirect trust, and

C_{N1}: trust weighted factor for the negative trust.

4.1.2 Example of assessing trust value for VER

Figure 7 shows the VERs and relations as an example of the trust evaluation sub-model for the VER. The example includes nine VERs ver_1, ver_2, …, ver_9, and specifically indicates some direct trusts, which can be used to assess the indirect and negative trusts, and thus obtain the trust value for the VER of ver_2 for ver_1 ($T_{ver}(ver_1, ver_2)$).

(Insert Fig. 7 Example of assessing trust value for VER)

From Fig. 7, the following is obtained

$DT_{ver}(ver_1, ver_2) = 0.56$

Using Functions 2 and 3 yields

$$IT_{ver_2}(ver_1, ver_2) = \frac{1 \times 0.8 + 1 \times 0}{2} = 0.4$$

$$IT_{ver_3}(ver_1, ver_2) = \frac{0.3 \times 0.45 \times 0.28}{1} = 0.0378$$

Assume that $\alpha_2 = 0.75$ and $\alpha_3 = 0.25$. Using Function 4 yields

$$IT_{ver}(ver_1, ver_2) = 0.75 \times 0.4 + 0.25 \times 0.0378 = 0.30945$$

From Fig. 7 and these relations among the VERs, we can infer that k=3 (including ver_3, ver_5 and $ver_{4\text{-}6}$), n=2 (including ver_7 and ver_8) and p=1 (including ver_9).

Substituting k, n and p into Function 6 yields

$$NT_{ver}(ver_1, ver_2) = \frac{0.2 + 1}{3 + 2 - 1} = 0.3$$

Based on the secure threshold of resource, set C_{D1}=0.7, C_{I1}=0.3 and C_{N1}=0.5.

Function 7 yields

$$T_{ver}(ver_1, ver_2) = 0.7 \times 0.56 + 0.3 \times 0.30945 - 0.5 \times 0.3 = 0.334835$$

The above mathematical manipulations yield $T_{ver}(ver_1, ver_2)$=0.334835. Considering the resource sharing among VERs in a project, ver_1 is authorized to access the resource owned by ver_2, while the resource threshold is equal to or below the calculated trust value for the VER.

4.2 Trust evaluation sub-model for project

The project relations defined in Section 2.2.3 can specifically indicate the operation mode of interaction among projects, enabling project resources to be shared or reused during the project lifecycle. Consequently, security for project resources is vital to project success. This sub-section describes a trust evaluation sub-model, resolving the difficulty of indefinite assignments across project boundaries.

4.2.1 Trust evaluation functions for Project

This sub-section initially defines terms concerning the trust evaluation sub-model for projects, and then presents some functions for assessing the level of trust of each project relation from one project to the others. As with the VER trust evaluation sub-model, three trust values are considered, defined as follows:

(1) *Direct Trust* from Project p_i to p_j, $DPT(p_i, p_j)$, is defined as the level of trustworthiness of p_j for p_i (See Fig.8) and is calculated from the project relations between p_i and p_j. The DPT is a positive correlation coefficient increasing the trust intensity with its increased value. The solid line between two projects in Fig. 8 denotes the direct trust for a project. Since various project relations enable different levels of resource sharing, the DPT is written as Function 9, which comprises five direct trust values for version, subset, process, reference and exclusive project relations, where the direct trust for exclusive project relation acts as a key gate for determining whether the DPT is 0 or greater than 0. Hence, Function 9 and the five direct trust functions defined in this sub-section clearly indicate that the direct trust function for project is in the range [0, 1].

(Insert Fig. 8 Part of Role Relation Net presenting the direct and indirect trusts for project)

$$\mathrm{DPT}(p_i, p_j) = \left[\left(\mathrm{DPT}_{\mathrm{version}}(\mathrm{p_i}, \mathrm{p_j}) + \mathrm{DPT}_{\mathrm{subset}}(\mathrm{p_i}, \mathrm{p_j}) + \mathrm{DPT}_{\mathrm{reference}}(\mathrm{p_i}, \mathrm{p_j}) + \mathrm{DPT}_{\mathrm{process}}(\mathrm{p_i}, \mathrm{p_j}) \right) \Big/ 4 \right] \times \mathrm{DPT}_{\mathrm{exclusive}}(\mathrm{p_i}, \mathrm{p_j}) \qquad (9)$$

Where

DPT(p_i,p_j): direct trust of p_j for p_i; and

$DPT_{version}$(p_i,p_j), $DPT_{subeset}$(p_i,p_j), $DPT_{reference}$(p_i,p_j), $DPT_{process}$(p_i,p_j) and $DPT_{exclusive}$(p_i,p_j) separately denote the direct trust of p_j for p_i at version, subset, reference, process and exclusive relations.

The five direct trust functions with various project relations are described in order, as follows:

- *Direct trust function for version project relation* from project p_i to p_j, $DPT_{version}(p_i, p_j)$, measures the trustworthiness intensity of project p_j for project p_i when considering the version project relation. The risk of accessing an unauthorized resource via the version relation might depend on the intersection of enterprise members from the two projects. Based on the above principle, the direct trust function for the version project relation is derived as Function 10, which is in the range [0, 1].

$$\mathrm{DPT}_{\mathrm{version}}(p_i, p_j) = \begin{cases} \dfrac{\left| FT_{ik}\, corresponding to FT_{jk} \right|}{\mathrm{Min}\{|\,\mathrm{FT_i}\,|, |\,\mathrm{FT_j}\,|\}} & \text{if } \exists (p_i R_{pv} p_j) \text{ and } \exists (EM_{im} \neq EM_{jn}) \\ 1 & \text{if } \exists (p_i R_{pv} p_j) \text{ and } \forall (EM_{im} = EM_{jn}) \\ 0 & \text{otherwise} \end{cases} \qquad (10)$$

Where

p_i: trustee project;

p_j: trusted project;

$DPT_{version}$(p_i,p_j): direct trust of p_j for p_i at version project relation;

FT_i: function tasks involved in p_i;

FT_j: function tasks involved in p_j;

$|FT_i|$: number of function tasks involved in p_i;

$|FT_j|$: number of function tasks involved in p_j;

$|FT_{ik}$ *corresponding to* $FT_{jk}|$: number of functional tasks assigned to p_i and linked to the functional tasks assigned to p_j via correspondence relations;

EM_{im}: enterprise members participating in project p_i;

EM_{jn}: enterprise members participating in project p_j, and

$p_iR_{pv}p_j$: version project relation between p_i and p_j.

- *Direct trust function for subset project relation* from project p_i to p_j, $DPT_{subset}(p_i, p_j)$, measures the trustworthiness of project p_j for p_i when considering a subset project relation. The risk of

accessing an unauthorized resource through a subset relation might depend on the amount of resources used by projects p_i and p_j. Therefore, the direct trust function for subset project relation can be obtained as Function 11, which is in the range [0, 1].

$$\mathrm{DPT}_{\mathrm{subset}}(p_i, p_j) = \begin{cases} \dfrac{\left|PublicP_i \cap PublicP_j\right|}{\mathrm{Min}\{|PublicP_i|, |PublicP_j|\}} & \text{if } \exists p_i R_{ps} p_j \\ 0 & \text{otherwise} \end{cases} \quad (11)$$

Where

$DPT_{subset}(p_i,p_j)$: direct trust of p_j for p_i at subset project relation;

$PublicP_i$: public resources assigned to projects p_i;

$PublicP_j$: public resources assigned to projects p_j;

$|PublicP_i|$: number of public resources assigned to projects p_i;

$|PublicP_j|$: number of public resources assigned to projects p_j;

$|PublicP_i \cap PublicP_j|$: number of public resources assigned simultaneously to projects p_i and p_j, and

$p_iR_{ps}p_j$: subset project relation between p_i and p_j.

- *Direct trust function for reference project relation* from project p_i to p_j, $DPT_{reference}(p_i, p_j)$, measures the trust intensity of project p_j for p_i when addressing the reference project relation. The risk of accessing an unauthorized resource using a reference relation is based on the enterprise members participating in the two projects or in other projects. Consequently, the direct trust function for the reference project relation can be determined as Function 12, which is in the range [0, 1].

$$\mathrm{DPT}_{\mathrm{reference}}(p_i, p_j) = \begin{cases} \dfrac{\left|EM_i \cap EM_j\right|}{Min\{|EM_i|, |EM_j|\}} & \text{if } \exists p_i R_{pr} p_j \\ 0 & \text{otherwise} \end{cases} \quad (12)$$

Where

$DPT_{reference}(p_i,p_j)$: direct trust of p_j for p_i at reference project relation;

$|EM_i|$ and $|EM_j|$: numbers of enterprise members participating in project p_i and p_j, respectively;

$|EM_i \cap EM_j|$: number of enterprise members simultaneously participating in projects p_i and p_j, and

$p_iR_{pr}p_j$: reference project relation between p_i and p_j.

- *Direct trust function for process project relation* from project p_i to p_j, $DPT_{process}(p_i, p_j)$, measures the trust intensity of project p_j for p_i when addressing the process project relation. The risk of accessing an unauthorized resource via a process relation might depend on the

workflow among the functional tasks involved in the two projects. Hence, the direct trust function for the process project relation can be derived as Function 13, which is in the range [0, 1].

$$\mathrm{DPT}_{\mathrm{process}}(p_i, p_j) = \begin{cases} \dfrac{|FunctionalTaskWorkflow|}{Min\{|FT_i|, |FT_j|\}} & \text{if } \exists p_i R_{pp} p_j \\ 0 & \text{otherwise} \end{cases} \quad (13)$$

Where

$DPT_{process}(p_i,p_j)$: direct trust of p_j for p_i at process project relation;

$|FunctionalTaskWorkflow|$: number of workflow relations among function tasks, which indicates the priority of functional tasks involved in the two projects, and

$p_iR_{pp}p_j$: process project relation between p_i and p_j.

- *Direct trust function for exclusive project relation* from project p_i to p_j, $DPT_{exclusive}(p_i, p_j)$, is utilized as a key gate to determine the final direct trust value from projects p_i to p_j. The $DPT_{exclusive}(p_i, p_j)$ is either 0 or 1, depending on whether an exclusive project relation is available. Accordingly, the direct trust function for exclusive project relation can be obtained as Function 14.

$$\mathrm{DPT}_{\mathrm{exclusive}}(p_i, p_j) = \begin{cases} 0 & \text{if } \exists p_i R_{pe} p_j \\ 1 & \text{otherwise} \end{cases} \quad (14)$$

Where

$DPT_{exclusive}(p_i,p_j)$: direct trust of p_j for p_i at exclusive project relation, and

$p_iR_{pe}p_j$: exclusive project relation between p_i and p_j.

(2) *Indirect Trust* from project p_i to p_j, $IPT(p_i, p_j)$, is defined as the level of trustworthiness of p_j for p_i via third-projects linked with one or both of p_i and p_j. The indirect trust for project is a positive correlation coefficient ranged between 0 and 1 to intensify the trust level between projects p_i and p_j, and derived from the project relations of third-projects with or without projects p_i and p_j. Figure 9 shows the part of an RRN denoting projects and project relations.The indirect trust function of a project at depth 2, based on the project's direct trust function, is derived as in Function 15 when the transitive property is available.

(Insert Fig. 9 Part of role relation net to present negative trust for project)

$$\mathrm{IPT}_2(p_i, p_j) = \sum_{l=1}^{k_2} \left[DPT(p_i, pI_l) \times DPT(pI_l, p_j) \right] \Big/ k_2 \quad (15)$$

Where

$IPT_2(p_i,p_j)$: indirect trust of p_j for p_i at depth 2;

$DPT(p_i,p_j)$: direct trust of p_j for p_i;

pI_l: third-project; and

k_2: number of third-projects that associate with p_i and p_j simultaneously, i.e., the number of paths from p_i to p_j via pI_l, $1 \le l \le k_2$.

Using the concept of Function 16 and referring the indirect trust function for VER at depth 3, the indirect trust function for projects at depths beyond 3 can be obtained. Owing to page space limits, this paper does not show the functions $IPT_3(p_i,p_j)$, $IPT_4(p_i,p_j)$, and beyond.

Consequently, the total indirect trust function for project is represented in Function 16, where, according to Eq. 17, each weight factor is in the range [0, 1] and the sum of the all weight factors must equal 1.

$$\mathrm{IPT}(p_i, p_j) = \sum_{w=2}^{\text{max-depth}} \beta_w \times IPT_w \qquad (16)$$

$$\sum_{w=2}^{\text{max-depth}} \beta_w = 1 \qquad (17)$$

Where

$IPT(p_i,p_j)$: total indirect trust of p_j for p_i;

β_w: trust weighted factor for indirect trust function at depth w, $2 \leqq w \leqq$ max-depth; and

max-depth: maximal depth of available transitive property.

(3) *Negative Project Trust Function* from project p_i to p_j, $NPT(p_i, p_j)$, is a negative correction coefficient in the range 0 and 1, and is applied to reduce the project trust intensity. Function 18 shows the negative trust function for project.

$$\mathrm{NPT}(p_i, p_j) = \sum_{m=1}^{n} DPT(pI_m, p_j) \Big/ (k + n - \mathrm{p}) \qquad (18)$$

Where

k: number of third-projects with project relations with projects p_i and p_j, simultaneously, and the number of indirect trust values from p_i to p_j (such as projects $p_{k1}, p_{k2}, \ldots, p_{kk}$);

n: number of third-projects which have subset, version, reference or process project relations with project p_j (such as projects $p_{m1}, p_{m2}, \ldots, p_{mn}$), and

p: number of third-projects which have an exclusive project relation with project p_j (such as projects $p_{n1}, p_{n2}, \ldots, p_{np}$).

Considering DPT, IPT and NPT, this study presents the trust function for projects as shown in Function 19, where C_{D2}, C_{I2} and C_{N2} denote three real coefficients used as weighted factors that can

be restricted with Equation 20. Different trust values for project are obtained by altering the three coefficients based on the project security policy.

$$PT(p_i, p_j) = C_{D2} \times DPT(p_i, p_j) + C_{I2} \times IPT(p_i, p_j) - C_{N2} \times NPT(p_i, p_j) \quad (19)$$

$$C_{D2}, C_{I2} \text{ and } C_{N2} = [o, 1] \quad (20)$$

4.2.2 Example of assessing trust value for project

Figure 10 shows an example of the project trust model, which considers ten projects (p_1, p_2, …, p_{10}) and various project relations. This example aims to assess the project trust value of p_2 from the perspective of p_1 ($PT(p_1, p_2)$). To simplify the illustration of the example, some direct trusts for project are assumed as displayed in Fig. 10.

(Insert Fig. 10 Example of calculating trust value for project)

From Fig. 10, Function 9 is applied to yield

$$DPT(p_1, p_2) = \frac{0 + 0.72 + 0 + 0.4}{4} \times 1 = 0.28$$

Using Function 15 yields

$$IPT_2(p_1, p_2) = \frac{0.6 \times 0 + 0.33 \times 0.2 + 0 \times 0.4}{3} = 0.022$$

In the example, only indirect trust for project at depth 2 is available, so that the total indirect trust equals to the indirect trust for project at depth 2.

Referring to Fig. 10 and calculating all project relations among projects, then k=3 (including projects p_3, p_4 and p_5), n=3 (including projects p_6, p_7 and p_8) and p=2 (including projects p_9 and p_{10}).

Substituting these integers into Function 18 yields

$$NPT(p_1, p_2) = \frac{0.6 + 0.45 + 0.3}{3 + 3 - 2} = 0.3375$$

Based on the threshold of project resource security and the restriction on Equation 20, set C_{D2}=0.7, C_{I2}=0.3 and C_{N2}=0.5.

Substituting these coefficients into Function 19 yields

$$PT(p_1, p_2) = 0.7 \times 0.28 + 0.3 \times 0.022 - 0.5 \times 0.3375 = 0.03385$$

The above mathematical manipulation yields the project trust value of p_2 from the perspective of p_1, $PT(p_1, p_2)$=0.03385. Considering the resource sharing across projects, project p_1 is authorized to access the resources owned by project p_2, while the secure threshold for the resources is equal or less than the project trust value.

4.3 An example of trust evaluations for virtual enterprise role and project

This sub-section uses Fig. 2 as an example to introduce the application of the proposed trust method. Table 1 lists three of all attributes of each functional task in Fig. 2.

(Insert Table 1 Attribute list of functional tasks)

Table 2 lists the project and VER thresholds of all public permission (resource).

(Insert Table 2 Threshold list of public permission)

Table 3 lists the assignments between VER and public permission.

(Insert Table 3 VER public permission assignment list)

In the example some states are set, including attributes, assignments, thresholds and trust for project and virtual enterprise role. Finally, we can decide each subject's authorizations based on trust values. While $DPT(p_1,p_2)$=0.35, $DPT(p_2,p_3)$=0.2, $DPT(p_1,p_3)$=-1, $T_{ver}(ver_{21}, ver_{22})$=0.5 and $T_{ver}(ver_{22}, ver_{21})$=0.6, the authorizations of each virtual enterprise role are listed in Table 4.

(Insert Table 4 VER authorization list after considering sharing and trusts)

5. Discussion and Conclusions

Resource management and sharing in collaborative virtual enterprise environment will in the future become increasingly complicated because of the need for information transparency. Based on the results of the requirements of resource sharing in virtual enterprise, this study proposed a VEAC-based trust evaluation method to resolve the issue of trust evaluation for sharing resources across enterprise and project boundaries.

5.1 Results and Contributions

The VEAC model can significantly simplify the explicit specifications and administration of access control in virtual enterprise by specifying the various relations among various elements,

while the trust evaluation method provides a secure mechanism for supporting VEAC's need for security and flexibility. The detailed results and contributions of this study are:

(1) The proposed trust evaluation sub-model for VER and the trust evaluation sub-model for project can measure the trust value among various VERs to facilitate the secure resource sharing across organization.
(2) The VEAC-based trust method can solve the drawback from the VEAC model and facilitate more securely and flexibility for resource sharing to support cross-organizational collaborative activities in virtual enterprises.
(3) With the change of each resource threshold, each resource's owner can frequently adjust the security level to adapt to various secure threats.
(4) This study may provide a suitable foundation for building a high-assurance trusted cooperative platform in dynamic virtual teams.

5.2 Further research

To develop a virtual enterprise access control mechanism for managing and facilitating resource sharing, some investigations need to be performed, and the following factors should be considered in future:

(1) This study only considered two elements of the VEAC model to develop the trust evaluation method; the other elements should be considered in the future.
(2) As well as direct, indirect and negative trust factors, other factors, such as the user's historical data, should be addressed to determine the level of trust and access resources and amount of referral from other trusted entities.
(3) This study does not consider that the user might share a resource with unauthorized users after legally acquiring it.
(4) Methods for the access control server to call and use resources in the heterogeneous platform were not addressed.
(5) An enterprise may participate in several competing VEs. Leaking of professional key technology or data should be prevented.
(6) Future studies may apply the XACML (eXtensible Access Control Markup Language) presented by OASIS to develop project access control policy frameworks to integrate access strategies among enterprises.
(7) VEAC model-based algorithms for generating user authorization are highly promising for use in supporting the virtual enterprise access control system.

Acknowledgment

This research is financially supported by National Science Council of the Republic of China

under Contract Nos: NSC94-2524-S-024-002, NSC94-2524-S-006-005 and NSC94-2524-S-006-006. NSC94-2525-S-343-001

References

[1] Chen YM, Liang MW. Design and implementation of a collaborative engineering information system for allied concurrent engineering. Int. J. of Computer Integrated Manufacturing 1999; 13(1):11-30.

[2] Ouzounis EK. An agent-based platform for the management of dynamic virtual enterprises. Ph.D Thesis; 2001.

[3] Park JS, Hwang J. RBAC for collaborative environments: Role-based Access Control for collaborative enterprise in peer-to-peer computing environments. Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies; 2003. p. 93-9.

[4] Kanet JJ, Faisst W, Mertens P. Application of information technology to a virtual enterprise broker: the case of Bill Epstein. International Journal of Production Economics; 1999, p. 23-32.

[5] Stephens B. Security architecture for system wide information management, Digital Avionics Systems Conference; 2005.

[6] Charles E, Phillips TC, Ting SAD. Information sharing and security in dynamic coalitions. Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies; 2002, p. 87-96.

[7] Zha X, Ding N. Study on information sharing in supply chain. Proceedings of the 7th International Conference on Electronic Commerce; 2005, p. 787-9.

[8] Li N, MitChell JC, Winsborough WH. Beyond proof-of-compliance: security analysis in trust management. Journal of ACM 2005; 52(3): 474-514.

[9] Biba KJ. Integrity considerations for secure computer systems. Bedford, MA: The MITRE Corporation; 1977.

[10] Frenkel A, Afsarmanesh H, Garita C. Hertzberger L.O. Supporting information access rights and visibility levels in virtual enterprise. IFIP TC5/WG5.3 Second IFIP working Conference on Infrastructures for Virtual Organizations: Managing Cooperation in Virtual Organizations and Electronic Business towards Smart Organizations; 2000.

[11] Kern A, Schaad A, Moffett J. Enterprise role administration: an administration concept for the enterprise Role-based Access Control Model. Proceedings of the eighth ACM Symposium on Access Control Models and Technologies; 2003, p. 3-11.

[12] Au R, Looi M, Ashley P. Automated cross-organizational trust establishment on extranets. Proceeding of Workshop on Information Technology for Virtual Enterprises; 2001, p. 3-11.

[13] Shand B, Dimmock N, Bacon J. Trust for ubiquitous, transparent collaboration. Proceedings of the First IEEE International Conference on Pervasive Computing and Communications; 2003, p. 153-60.

[14] Tran H, Hitchens M, Varadharajan V, Watters P. A trust based access control framework for

P2P file-sharing systems. Proceedings of the 38th Hawaii International Conference on System Seciences; 2005, p. 302c-302c.

[15] Dimmock N, Belokosztolszki A, Eyers D. Using trust and risk in role-based access control policies. SACMAT; 2004, p. 156-62.

[16] Barrett S, Konsynski B. Inter-organization information sharing systems. MIS Quarterly; 1982, p. 83-105.

[17] Zuo Y, Panda B. Component based trust management in the context of a virtual organization. ACM Symposium on Applied Computing; 2005, p. 1582-8.

[18] Ahn, G.J. Specification and classification of role-based authorization policies. Twelfth IEEE International Workshops; 2003, p. 202–7.

[19] Wang CB, Chen TY, Chen YM, Chu HC, Yang H. Access control requirements and model for resource management and sharing in virtual enterprise. Automation Conference; 2005.

[20] Al-Kahtani MA, Sandhu R. A model for attribute-based user-role assignment. Computer Security Applications Conference 18th Annua; 2002, p. 353–62.

[21] Botha RA, Eloff JHP. Designing role hierarchies for access control in workflow systems. Computer Software and Applications Conference; 2001, p. 117–22.

[22] Dridi F, Muschall B, Pernul G.. Administration of an RBAC system. Proceedings of the 37th Annual Hawaii International Conference; 2004, p. 187–92.

[23] Kern A, Schaad A, Moffett J. Enterprise role administration: an administration concept for the enterprise role-based access control model. Proceedings of the eighth ACM Symposium on Access Control Models and Technologies; 2003, p. 3-11.

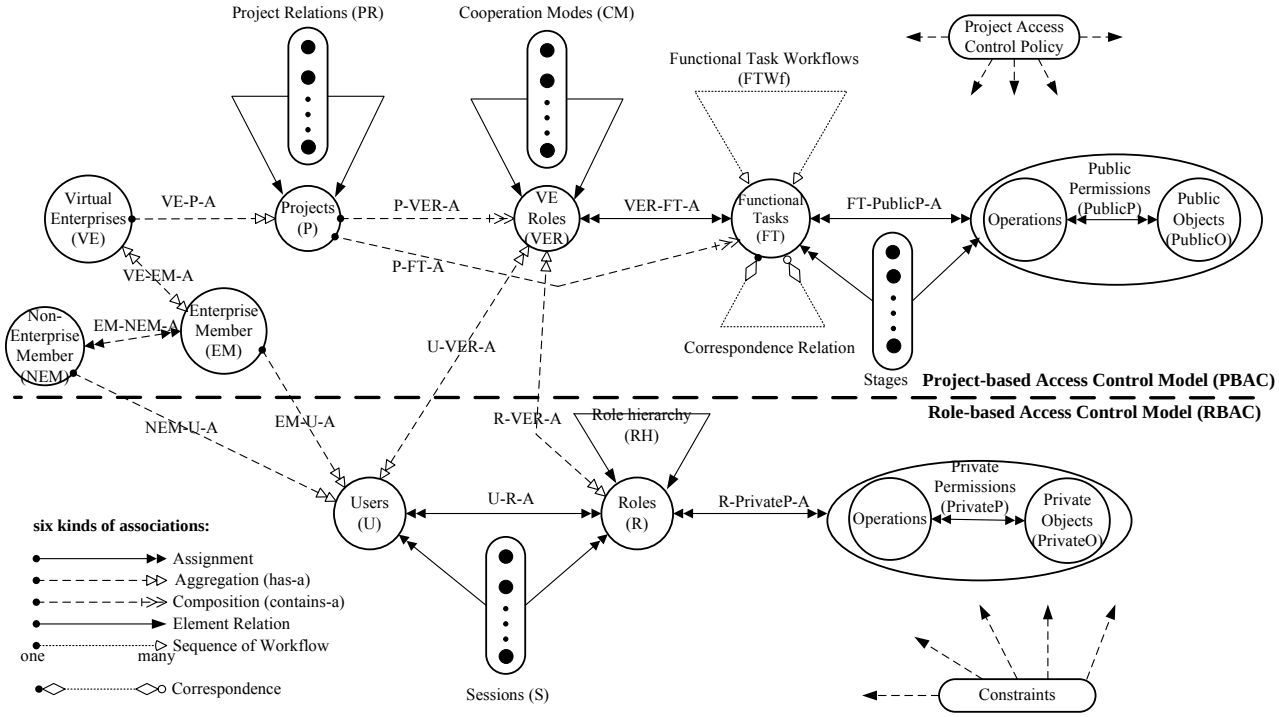
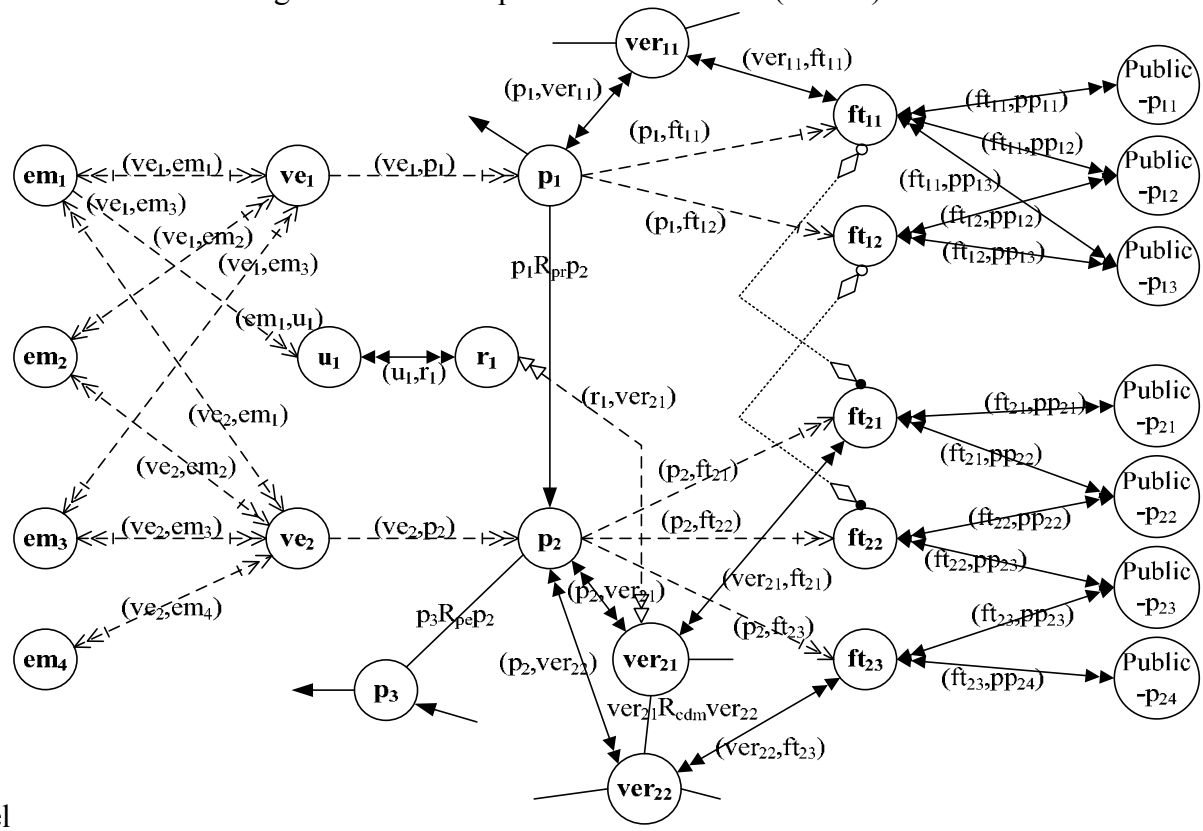


Fig. 1 Virtual Enterprise Access Control (VEAC)



Model

Fig. 2 Part of a Role Relation Net (RRN)

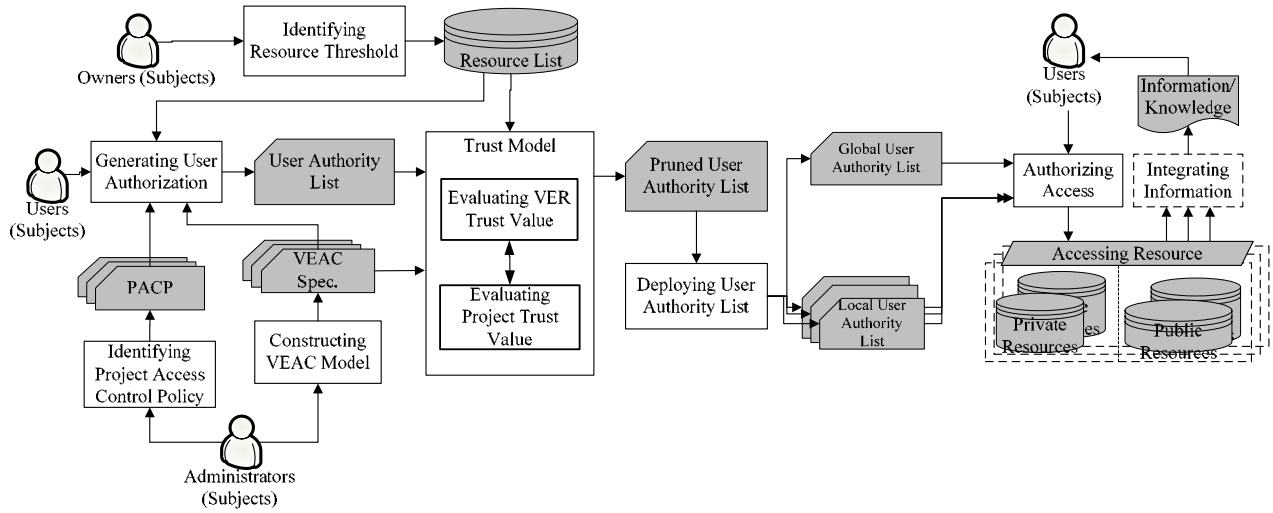


Fig. 3 Access control framework in a virtual enterprise

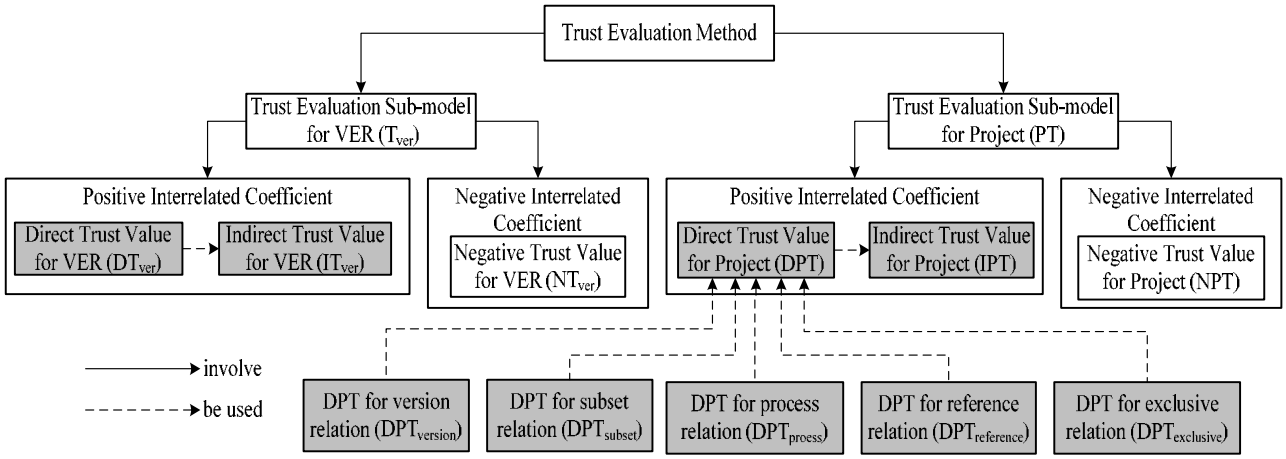


Fig. 4 Structure of the trust evaluation method

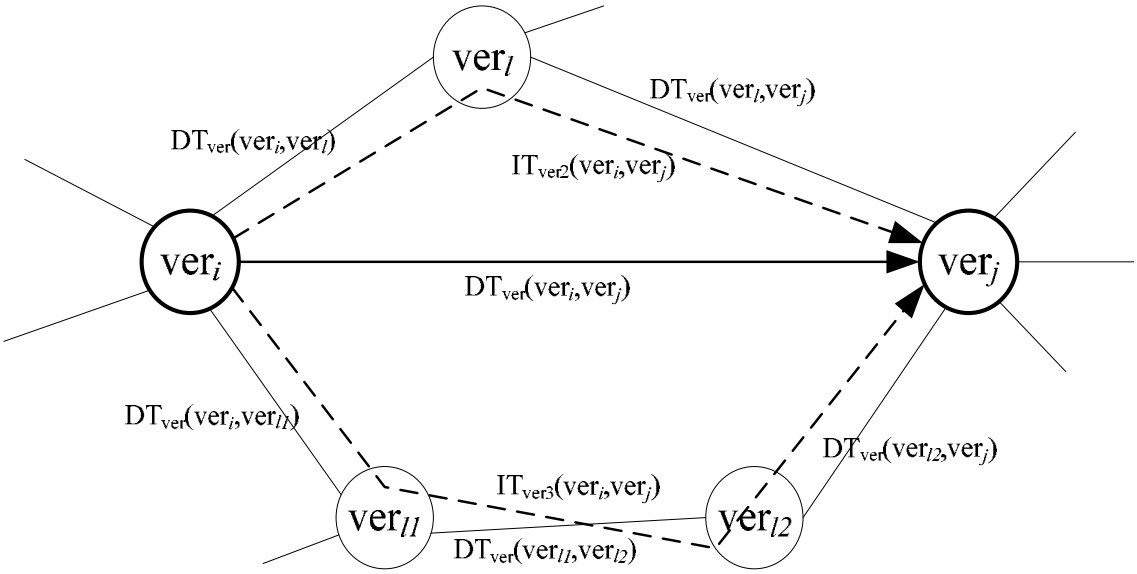


Fig. 5 Part of Role Relation Net (RRN) denoting the direct and indirect trusts for VER

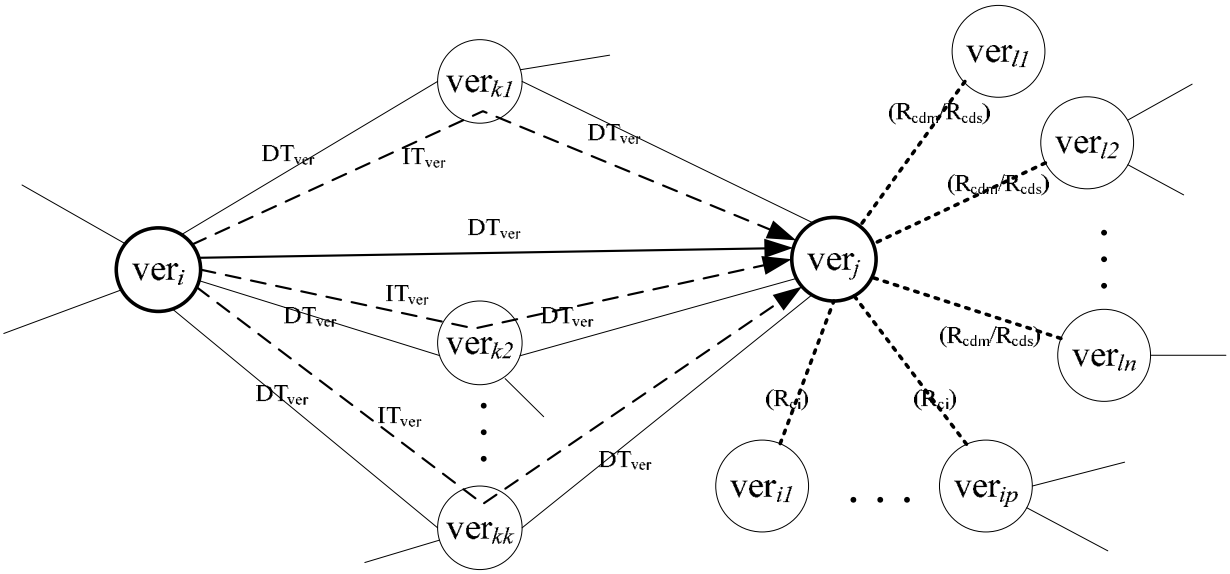


Fig. 6 Part of Role Relation Net (RRN) representing the negative trust for VER

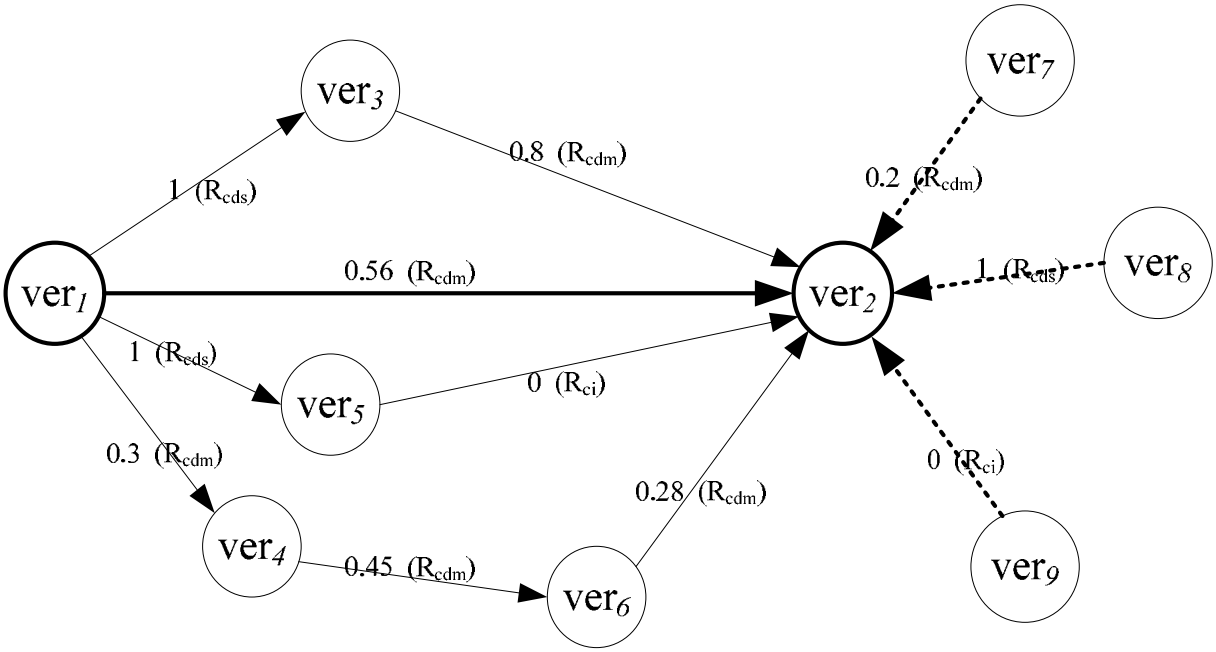


Fig. 7 Example of assessing trust value for VER

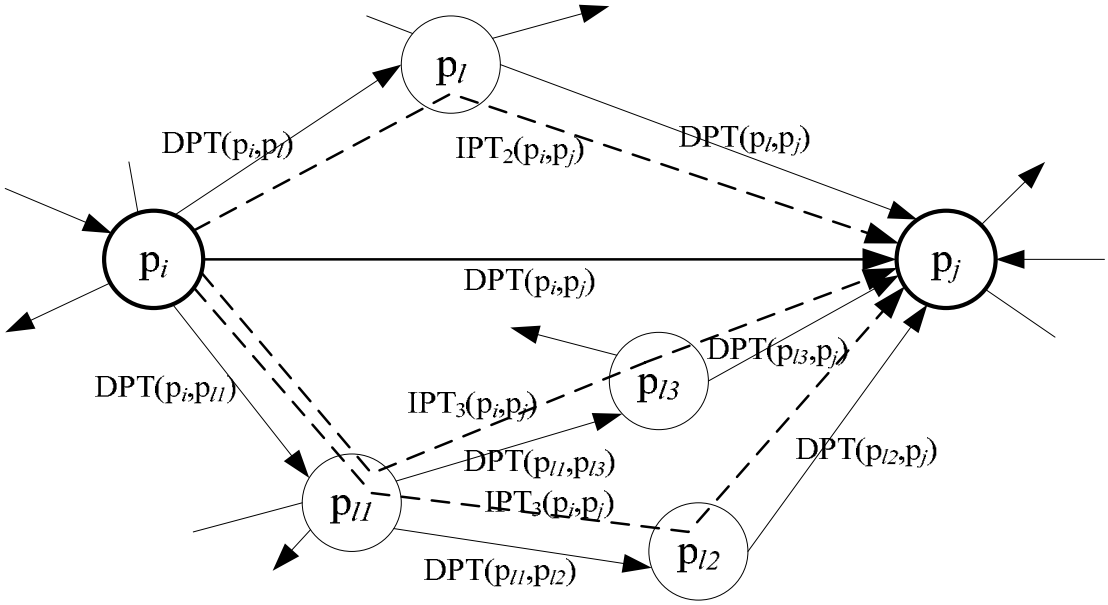


Fig. 8 Part of Role Relation Net presenting the direct and indirect trusts for project

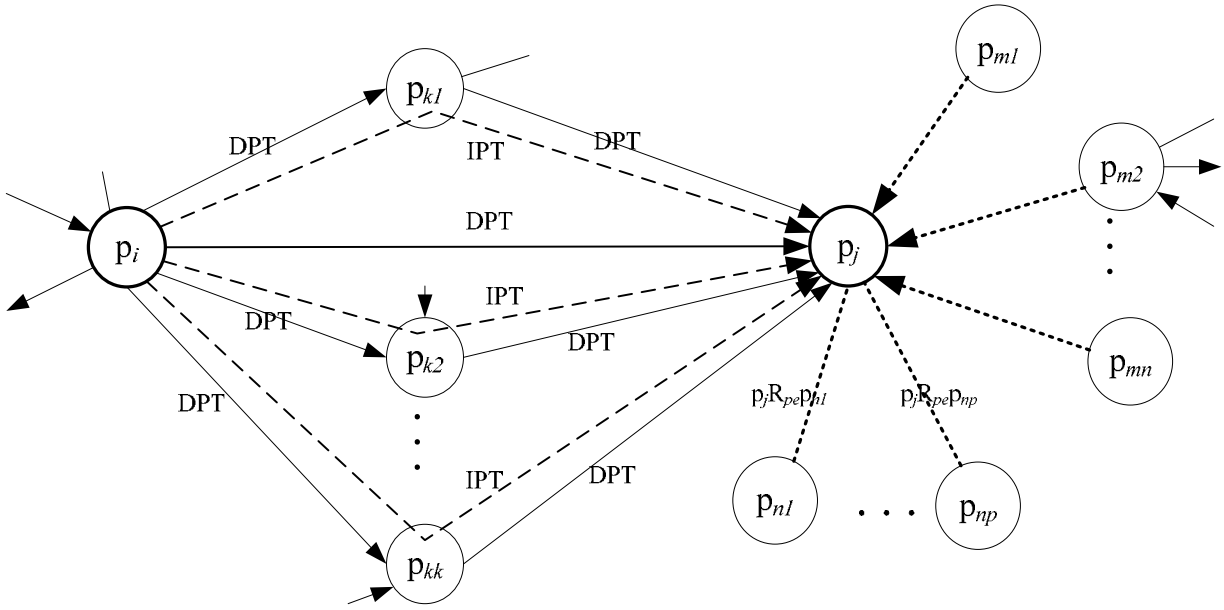


Fig. 9 Part of role relation net to present negative trust for project

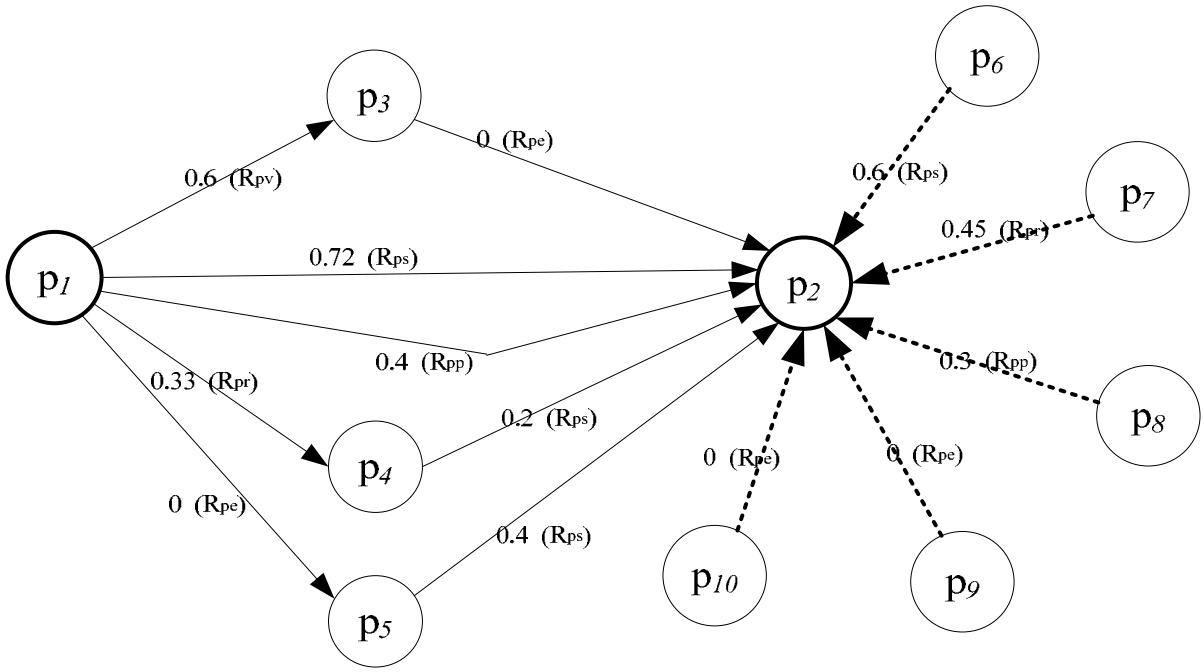


Fig. 10 Example of calculating trust value for project

Functional Task (FT)	**Attributes**		
	Allowed-reference	**Allowed-sub-project**	**Allowed-main-project**
ft_{11}	F	F	F
ft_{12}	T	T	F
ft_{21}	T	T	T
ft_{22}	T	T	T
ft_{23}	T	F	F

Table 1. Attribute list of functional tasks

Public Permission (Resource)	**Threshold of Project**	**Threshold of Virtual Enterprise Role**
public-p_{11}	0.7	0.8
public-p_{12}	0.62	1
public-p_{13}	0.2	1
public-p_{21}	0.1	0.7
public-p_{22}	0.22	0
public-p_{23}	0.35	0
public-p_{24}	0.4	0.6

Table 2. Threshold list of public permission

Virtual Enterprise Role (VER)	Public Permission (Resource)
ver_{11}	public-p_{11}, public-p_{12}, public-p_{13}
ver_{21}	public-p_{21}, public-p_{22}
ver_{22}	public-p_{23}, public-p_{24}

Table 3. VER public permission assignment list

Virtual Enterprise Role (VER)	Public Permission (Resource)
ver_{11}	public-p_{11}, public-p_{12}, public-p_{13}
ver_{21}	public-p_{21}, public-p_{22}, public-p_{23}
ver_{22}	public-p_{23}, public-p_{24}, public-p_{22}

Table 4. VER authorization list after considering sharing and trusts