合作式代理人對機密性資訊存取機制之研究

林忠毅[1] 林鳳儀[2*] 方自億[3] 甯方璽[4]

[1]國防大學資訊管理系
[2]國立臺北科技大學經營管理系
[3]國立臺北科技大學工商管理研究所
[4]軍備局生產製造中心測量隊

摘 要

資訊科技除了帶來許多正面效益，相對地，也帶來許多負面的影響。就具機敏性資料庫存取而言，若未有任何安全機制，攻擊者欲竊取資料，如同進入無人之境；即使資料庫存取，具有完善權限密碼機制，也無法防範管理者監守自盜或密碼遭竊取風險。故本研究以代理人環境結合「互動式識別方法」、「門檻方法」機制，達成二階層式的資料防護及遠端資料庫管理人員間相互認證，並透過門檻機制，當達到門檻人數，才能將資料庫解開，以解決單一管理鑰匙可能衍生之威脅。

關鍵詞：代理人，互動式識別方法，門檻方法，機密性資訊

The Study of Classified Information Access with a Collaboration Agent Scheme

Zhong-Yi Lin [1],Fengyi Lin [2*], Tzu-Yi Fang [3], and Fang-Shii Ning[4]

[1] *Management College, National Defense University*
[2] *Department of Business Management , National Taipei University of Technology*
[3] *Industrial and Business Management , National Taipei University of Technology*
[4] *Base Survey Battalion, Materiel Production Center , Armaments Bureau*

ABSTRACT

Information technology not only has provided us countless positive benefits, on the contrary, also has brought us lots of negative effects. Take classified information for example, if the files are kept without any security protection, hackers can easily gain access to it. Nevertheless, even if the data is encrypted with password and other protection, it's still hard to avoid the risk the corruptive administrator from stealing the files.Thus, this research applies the Interactive Identification Scheme and the Threshold Scheme in the agent's procedure, which may develop the system into a 2-layer protection and create a mutual remote database administrator authentication. Through the use of Threshold Scheme, the access of the database can only decoded only if the threshold of administrators or agents are adequate. This way, the protract risk of only a singular administrator can be solved.

Keywords: annular reverse-flow combustor, inlet pressure, swirl intensity

文稿收件日期 98.5.1;文稿修正後接受日期 99.9.14;*通訊作者

Manuscript received May 1, 2009; revised September 14, 2010; * Corresponding author

一、前　言

資訊科技除了帶來許多正面效益，相對地，也帶來許多負面的影響；當使用者愈依賴它，就愈擺脫不了它。為避免造成利用資訊科技而造成更大損失，不論是企業組織、政府及軍事機關，在導入資訊科技前，必須先審慎考慮資訊科技應用於組織中所可能造成安全問題。就具機密性資料庫存取而言，若未有任何安全機制，攻擊者欲竊取資料，如同進入無人之境；即使資料庫存取，具有完善權限密碼機制，也無法防範使用者將密碼洩漏或於傳送過程中遭竊取。

隨著網路發展，企業組織規模由區域化轉變成全球化；為滿足全方位決策需求，企業組織建構整合各區域、部門資訊之資料倉儲，提供終端使用者存取所需之資訊，為現代化組織在競爭激烈環境中生存刻不容緩的要務。然而，資料倉儲內包含許多客戶訂單、行銷策略等機敏性資訊，誠如 Briney[1]在“Security Focused”文章中提及：「企業組織即使有良好的公鑰系統和加密技術，若未對終端使用者認證，整個資訊系統安全策略將會失敗」。

基於此，本研究建立代理人相互合作驗證環境，使用者與資料管理權限者僅須將驗證參數以明文方式，傳送至驗證伺服器，即可離線；驗證伺服器則透過各代理人間相互合作，達到彼此間身份確認，決定是否將資料庫開啟。此外，為了避免單一密鑰因被竊取，導致遭冒名攻擊及重要資訊外洩之風險，本研究採用門檻方法，使用者若需存取資料，需具其他相同存取權限之使用者同意，方能真正取得機密資訊存取權。

二、文獻探討

2.1代理人特性

Wang et al.[2]提出代理人在特定情況，具有運算處理能力，並且能決定本身的行動；同時它具有協調、談判與合作等社會能力；郭木興[3]認為代理人是一種新的程式編碼方式，可以處理複雜且單一程式不易或無法完成的工作。

Ferber[4]依代理人不同的目標與技術，大略區分成：

1、行動代理人（Mobile Agent）

行動代理人不必與服務主機溝通，便能在各服務主機遷移（Migrate），並且，往下個服務主機平台遷移前，能夠將搜尋的資料保存，最後將資料傳回給使用者。其主要特性為遠端分散式處理、非同步資料傳輸方式及整合異質系統平台資料等。

2、合作代理人（Collaborating Agent）

合作代理人系統在架構上，由數個代理人所組成，依賴彼此間合作與訊息的交換完成任務。

3、智慧型代理人（Intelligent Agent）

能從以往的經驗與需求中，觀察與學習使用者習慣的能力，並具有監視、推論與解釋事件的能力。

本研究為透過代理人相互間的合作，達到身份確認的功能，因此採用合作代理人方式，藉由彼此間分工合作完成共同目標。

2.2 代理人安全方面應用

Shakshuki 等學者[5]提出以代理人為基礎之安全服務方法。該研究架構採用集中式資源(安全性服務)控管，透過代理人彼此間合作、協調機制，建立安全的服務存取環境。其安全性服務環境架構由介面代理人(Interface Agent，IA)、認證代理人(Authentication Agent，ATA)、授權代理人(Authorization Agent，AUA)及服務提供代理人(Service Provider Agent，SPA)組成，其主要流程為：使用者提出服務需求時，透過 IA 將使用者相關訊息(使用者名稱、密碼及 Domain)傳送至 ATA，ATA 除了檢查使用者名稱及密碼外，並採用 Keystroke 分析及類神經網路(Neural Network)的方式，驗證使用者輸入資訊之時間間隔，俟驗證成功後發送訊息至 AUA。AUA 根據使用者 Domain，區分 local 及 foreign 驗證方式，並決定是否授權使用者存取需求。SPA 依據 AUA 訊息，提供使用者安全服務。

Lin [6]等學者，提出較具效率之存取控制及金鑰管理方法應用於行動代理人，避免其遷移過程中遭未經授權者存取。其方法為採用歐基里德演算法(Euclidean Algorithm)、尤拉定理(Euler's Theorem)等方法，產生解密鑰匙，並透過指數函數產生超級鑰匙，用以推導解密鑰匙，如圖 1 所示。

圖 1 中 SK_i 為超級鑰匙，可推導出符合其

權限之解密鑰匙，如擁有 SK_1 鑰匙者，可推導 DK_1 至 DK_4 之解密鑰匙；擁有 SK_3 鑰匙者，可推導出 DK_2 至 DK_4 之解密鑰匙。就行動代應用方面，代理人擁有者將不同權限的超級鑰匙 SK_i 分送給各節點 N_i，當代理人須至各節點主機遷移交易時，各節點可利用超級鑰匙推算其所屬的密鑰。

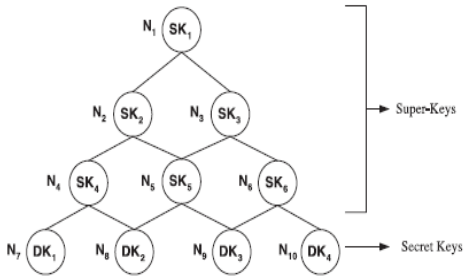

圖 1.密鑰推導之階層式架構。

Shakshuki 等學者提出方法(以下簡稱為 Shakshuki 等方法)與本研究均為透過代理人合作達成資料存取控制，然其身份認證方法卻是不同，Shakshuki 等方法除透過比對使用者名稱及密碼外，更須透過統計及類神經網路方式驗證使用者輸入的時間間隔成功後，方能完成身份確認；而本研究透過非對稱式密碼方式達到身份認證功能。

就 Shakshuki 等方法而言，使用者名稱與密碼並未加密保護，於網路上傳送時，易遭直接窺探及竄改風險，縱有後續輸入時間間隔比對，無法確保冒名攻擊之風險，此外，亦無法防止使用者事後否認交易之事實。

本研究利用非對稱式密碼方式，就功能性而言，除可確保使用者資料網路傳送時的完整性，更可防止使用者事後否認交易之事實。

2.3 門檻方法

Shamir[7]及 Blakley[8]於 1979 年利用 Lagrange 多項式插入法，提出一種秘密分享的方法，該方法又稱之為門檻方法，其中重要的二個參數為，門檻值(Threshold Value) t 及次密鑰的數目 n，一般以(t,n)來表示；此方法主要由 Dealer(本文定義為密鑰中心)，選定主密鑰 K，並打造不同次密鑰，讓每位參與者獲得一把次密鑰。因而當次密鑰的數目大於門檻值 t 時，便可推導主密鑰，反之，當次密鑰的數目小於門檻值 t 時，便無法推導主密鑰，亦即，當參與者有 10 人(次密鑰十把)，若門檻值 t=3，必須要具備三個參與者以上次密鑰方能推導主密鑰，該方法運作流程如下：

1、 密鑰中心 (Key Authentication，KAC)選擇一質數p及主密鑰K，且P≧K

2、 密鑰中心選擇t-1次方之多項式：

$$h(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+...K \bmod p \qquad (1)$$

3、 參與者向KAC註冊後，KAC依據各用戶之獨特識別碼 I_i 依(2)產生不同次密鑰。

$$K_i=h(I_i) \qquad i=1,2,3...,n \qquad (2)$$

4、 當超過門檻值t的次密鑰擁有者，KAC可依據(3)式還原主密鑰。

$$h(x)=\sum_{s=1}^{t}K_{is}\prod_{j=1,j\neq s}^{t}\frac{X-I_{il}}{I_{is}-I_{il}} \bmod p \qquad (3)$$

2.4 門檻式代理簽章相關文獻探討

Hwang[9]等學者，提出基於 RSA 密碼系統之門檻式代理簽章方法，該方法透過 Lagrange 方程式，分享代理簽署鑰匙，並應用 RSA 密碼系統取代傳統較大的密碼技術，提升整體效率，該研究實行過程依序為代理鑰匙分享、代理簽章使用及驗證等三階段，詳細說明如下：

2.4.1 前置階段

P_0 代表原始簽章者，$P_1,P_2,...,P_n$ 為 n 個代理簽章者，N_i 為 RSA 的模數，為大質數 p_i,q_i 之積，$N_i=p_i*q_i$，d_i 為 $P_{i,i=0\sim t}$ 之密鑰，e_i 為其公鑰，並滿足 $d_i*e_i=1 \bmod \phi(N_i)$，其中 $\phi(N_i)=(p_i-1)*(q_i-1)$，$N_i$ 及 e_i 可以被公開，但 d_i 及 $\phi(N_i)$ 必須秘密保存。m_w 為原始簽章者授權訊息，其中包含重要的資訊(如代理鑰匙的期限及代理簽章者身份等)。

2.4.2 代理鑰匙分享階段

假設原始簽章者 P_0 簽署授權訊息給 n 個

代理簽章者，須先產生群體代理簽章鑰匙 D 及代理簽章驗證鑰匙 E，如方程式(4)、(5)；隨之，P_0 將$\{m_w, E, [m_w \| E]^{d_0} \bmod N_0\}$公開。

$$D = {d_0}^{m_w} \bmod \phi(N_0) \quad (4)$$

$$E = {e_0}^{m_w} \bmod \phi(N_0) \quad (5)$$

P_0 隨機產生秘密 n-1 階多項式，如方程式(6)，其中$a_1, a_2, \cdots, a_{t-1}$均為隨機數， P_0 並依(6)產生各代理簽章者之簽署鑰匙$k_i = f(i)$，並將$[[k_i]^{d_0} \bmod \phi(N_0) \| k_i]^{e_i} \bmod N_i$傳送給代理簽章者$P_i$。

$$f(x) = D + a_1 x + \cdots + a_{t-1} x^{t-1} \bmod \phi(N_0) \quad (6)$$

各代理簽章者用其私鑰d_i將訊息解開，並用原始簽章者的公鑰e_0驗證k_i有效性，代理簽署鑰匙k_i 須秘密保存。

2.4.3 代理簽章使用階段

假設代理簽章者$P_{i,i=1\sim n}$欲使用$k_{i,i=1\sim n}$ 共同簽署訊息 M，其運算方式如方程式(7)、(8)，運算完成後，各代理簽章者將$\{[s_i]^{d_i} \bmod N_i, s_i\}$傳送給代理簽章匯整者(Combiner)

$$S_i = M^{(L_i * K_i)} \bmod N_0 \quad (7)$$

$$L_i = \prod_{i, j \in T, j \neq i} \frac{-j}{i-j} \quad (8)$$

代理簽章匯整者利用P_i之公鑰e_i驗證，若所有的簽章是有效的，則利用方程式(9)產生簽署於訊息 M 上之代理簽章 S(含有所有代理簽章者簽署鑰匙)。並將 S 傳送給驗證者。

$$\begin{aligned} S &= \prod_{i \in T} s_i \bmod N_0 \\ &= M^{\sum_{i \in T} L_i * f(i)} \bmod N_0 \\ &= M^{f(0)} \bmod N_0 \\ &= M^{D} \bmod N_0 \end{aligned} \quad (9)$$

2.4.4 代理簽章驗證階段

驗證者收到代理簽章 S 後，先以原始簽章者的公鑰運算m_w及 E 是否於授權期間，若授權期已屆滿，則代理驗證鑰匙 E 是無效的。當驗證成功後，驗證者使用(10)檢查代理簽章 S 有效性。

$$\begin{aligned} S^E \bmod N_0 &= (M^D)^E \bmod N_0 \\ &= M^{d_0 {}^{m_w} * e_0 {}^{m_w}} \bmod N_0 \\ &= M \bmod N_0 \end{aligned} \quad (10)$$

Wang[10]等學者，針對 Hwang 等學者方法，從私密性(secrecy)、代理簽章防護(Proxy Protection)、不可否任性及確認簽章(Non-Repudiation、Known singer)及不可偽造性(Unforgeability)提出以下缺點：

2.4.4.1 私密性：

(1)若門檻值以上之所有代理簽章者共謀，可得到代理簽章鑰匙 D。

(2)原始簽章者私鑰，具有被代理簽章者揭露之風險；透過$ED = 1 \bmod \phi(N_0)$，可推導 ED-1 為$\phi(N_0)$的倍數，代理簽者便藉由 N 推算出$\phi(N_0)$，再透過歐幾里德(EUCLIDEN)演算法，推算出原始簽章者私鑰。

2.4.4.2 代理簽章防護

基於所有代理簽署鑰匙$k_{i,i=1\sim n}$、群體代理簽章鑰匙 D 及代理簽章驗證鑰匙 E，均由原始簽章者產生，故可任意產生訊息，並透過方程式(9)直接運算 S，並交給驗證者；驗證者僅透過方程式(10)，檢查是否符合，並未檢查各代理簽章者是否動用過自己的私鑰，故原始簽章可偽造群體簽章過的訊息。

2.4.4.3 不可否認性及確認簽章者

由於代理簽章者間可能的共謀，可推導出群體代理簽章鑰匙 D；同樣地，原始簽章者也可透過 D 偽造訊息，直接傳送給驗證者，故代理簽章匯整者(Combiner)並無法發生真正功效，若未來發生爭端時，應由誰來負責？此外，因代理簽章匯整者(Combiner)並未擁有原始簽章者及代理簽章者簽章記錄，故原始簽章者及代理簽章者能夠事後否認簽章事實。

2.4.4.4 不可偽造性

基於 E、e_0及m_w是公開值，故外部非法

人員藉由 $e_0^{m_w} - E$ 得知其值為 $\phi(N_0)$ 的倍數，並分解原始簽章者之模 N_0 ，進而推導其私鑰，便可執行偽造攻擊。

三、機密性資訊存取機制

藉由 Shakshuki 等方法探討，其雖可達到身份驗證功能，然就安全性而言，缺乏資料傳送完整性及使用者不可否認性功能。

基於此，本研究採用非對稱式密碼方式，除可達到身份驗證功能，更具備資料傳送完整性及使用者不可否認性功能。

此外，為避免單一密鑰被竊取，而導致遭冒名攻擊及重要資訊外洩之風險，本研究透過門檻設定，改善單一密鑰遭竊取之風險。

3.1 驗證參數及代理人功能說明

本研究定義所有成員均具機密資料存取權限，為方便識別，成員中現行需存取機密性資料者，稱為使用者，餘為管理者。依 Shamir 門檻方法，本研究假設門檻值為 3；驗證參數及驗證方各代理人功能說明如表 1、表 2。

表 1. 驗證參數說明。

驗證參數	功能說明	公開與否
x_{au}	驗證方私鑰	否
y_{au}	驗證方公鑰	是
$x_{i=a,b,c}$	使用者及管理者私鑰	否
$y_{i=a,b,c}$	使用者及管理者公鑰	是
$w_{i=a,b,c}$	使用者及管理者產生之驗證子，讓驗證方驗證其身份	是
$r_{i=a,b,c}$	使用者及管理者產生之隨機值，為代理密鑰加密用	否
$t_{i=a,b,c}$	使用者及管理者產生之隨機值，為用於與密鑰結合，避免密鑰遭窺探之風險	否
n	使用者與管理者間之通訊碼	是
$c_{i=a,b,c}$	利用 y_i 產生加密值，用於驗證方推導，代理密鑰用	是
$e_{i=a,b,c}$	利用 t_i 產生加密值，用於驗證方推導，代理密鑰用	是
$valk_{i=a,b,c}$	使用者及管理者產生之代理密鑰，讓驗證方驗證其身份	否

表 2. 驗證方各代理人功能說明。

代理人名稱	功能
接收代理人	1.將使用者及管理者訊息解密。 2.將解密後代理密鑰交各代理人。
使用者代理人	1.代理所屬使用者或管理者驗證另二方身份。 2.驗證傳送過程是否遭到攻擊。
任務代理人	1.確認各代理人是否均完成驗證。 2.產生次密鑰。
資料擷取代理人	將次密鑰還原與原認證函數比對是否相符。

3.2 驗證伺服器各代理人合作驗證流程

本研究驗證流程，藉由各代理人間相互合作達成身份確認，如圖 2。

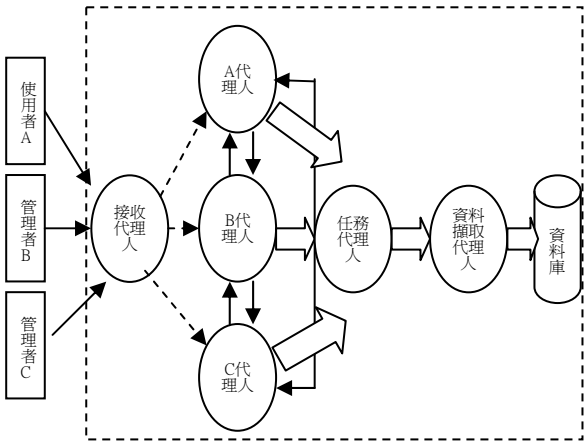

圖 2. 機敏性資訊存取架構。

驗證順序為藉由接收代理人接收使用者與管理者之驗證參數，並解出代理密鑰分別交給所屬代理人，以互相驗證彼此身份；當使用

者與管理者相對應之代理人(A、B及C代理人)代理人確認另二方身份成功後，則各自產生隨機值，交任務代理人；任務代理人收到使用者代理人隨機值，視同身份驗證通過，並檢查筆數是否達到三筆，若相符，則產生次密鑰交資料擷取代理人；資料擷取代理人先檢查次密鑰是否有三筆，若相符，則透過 Lagrange 公式導得一多項式，並與認證方程式比較，若相符，則開啟機密性資料庫，驗證模式詳細說明如下：

1、假設KAC公佈質數p、原根g及驗證方擁有認證函數$h(x)$，使用者及驗證方依據p、g利用本身的私鑰x_i及x_{au}，依(11)及(12)產生公鑰y_i、y_{au}，並將公鑰公開。

$$y_i = g^{x_i} \bmod p \quad _{i=a,b,c} \tag{11}$$

$$y_{au} = g^{x_{au}} \bmod p \tag{12}$$

2、假設存取資料同意門檻值必須達三人(包含使用者本人)，亦即A欲擷取資料，須經具管理權限者同意。假如A請求組織內成員B及C同意資料存取，並告知通訊碼n；當B、C同意A存取資料，彼此均先產生隨機值 ，並依(13)及(14)產生驗證子及代理密鑰；代理密鑰利用t_i及通訊碼n結合本身私鑰 ，除可避免私鑰直接遭窺探風險，驗證方更可利用相對公鑰驗證身份。

$$w_i = g^{t_i} \bmod p \quad _{i=a,b,c} \tag{13}$$

$$val\_k_i = t_i + x_i n \bmod \phi(p)_{i=a,b,c} \tag{14}$$

其中$\phi_1(p) = p-1$，為小於 p，且與 p 互質的正整數個數。

3、當完成驗證子及代理密鑰後，產生隨機值$r_{i,i=a,b,c}$，並依(15)產生$c_{i,i=a,b,c}$及依(16)利用驗證方公鑰及隨機值 將代理密鑰加密。

$$c_i = g^{r_i} \bmod p \quad _{i=a,b,c} \tag{15}$$

$$e_i = val\_k_i * y_{au}{}^{r_i} \bmod p \quad _{i=a,b,c} \tag{16}$$

4、A、B、C將$(w_i, n, c_i, e_{i,i=a,b,c})$傳送給驗證方之接收代理人，當三人訊息到達後，接收代理人利用密鑰依(17)及(18)求出代理密鑰。

$$(c_i)^{x_{au}} = (g^{r_i})^{x_{au}} = (g^{x_{au}})^{r_i} = y_{au}{}^{r_i} \bmod p_{i=a,b,c} \tag{17}$$

$$e_i (y_{au}{}^{r_i})^{-1} = val\_k_i * y_{au}{}^{r_i} * y_{au}{}^{-r_i} \bmod p = val\_k_j \bmod p \quad _{i=a,b,c} \tag{18}$$

5、當接收代理人求出A,B,C代理密鑰，將$(w_i, n, val_k_j)_{i=j=a,b,c}$傳送給所屬代理人，並依(19)~(21)代為驗證彼此身份，若結果相符，可確認為合法使用者或管理者，否則即為非合法人員或合法人員偽造訊息，系統便不執行後續程序。

A代理人：

$$g^{(val\_k_b + val\_k_c)} = w_b * w_c * y_b{}^n * y_c{}^n \bmod p \tag{19}$$

B代理人：

$$g^{(val\_k_a + val\_k_c)} = w_a * w_c * y_a{}^n * y_c{}^n \bmod p \tag{20}$$

C代理人：

$$g^{(val\_k_a + val\_k_b)} = w_a * w_b * y_a{}^n * y_b{}^n \bmod p \tag{21}$$

6、當各代理人驗證成功後，便替所屬人員產生隨機值$I_{i\ i=a,b,c}$傳送給任務代理人。

7、當任務代理人收到隨機值$I_{i\ i=a,b,c}$，先檢查筆數是否有三筆，若不符合，則表示代理人驗證非全數通過，故不採取後續程序；若相符，則將隨機值代入認證方程式$h(x)$，依序轉換成次密鑰：

$$h(I_a) = k_a \tag{22}$$

$$h(I_b) = k_b \tag{23}$$

$$h(I_c) = k_c \tag{24}$$

8、任務代理人再將各隨機值及次密鑰$(I_i, k_{ii=a,b,c})$，傳送給資料擷取代理人。

9、資料擷取代理人先檢查次密鑰是否有三筆，若不符合，則不執行後續程序，若相符，則依(25)驗證利用次密鑰所計算之函數$h_1(x)$是否與認證方程式$h(x)$符(26)，若相符，資料擷取代理人開啟資料庫，反之則拒絕將資料庫開啟。

$$h_1(I_i) = \sum_{s=1}^{t} K_{is} \prod_{j=1, j\neq s}^{t} \frac{X - I_{jl}}{I_{is} - I_{il}} \bmod p \tag{25}$$

$$h_1(I_i) \stackrel{?}{\equiv} h(x) \tag{26}$$

3.3代理人自主性驗證機制

本研究驗證伺服器之各代理人接受任務委託後，便自主性執行任務，詳如圖 3 所示。

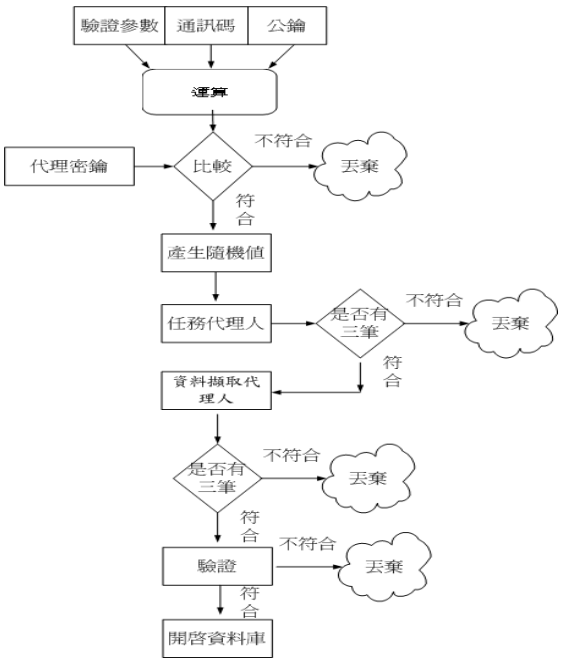

圖 3.各代理人自主性驗證機制圖。

使用者代理人(A、B、C代理人)接收到 $(w_i,n,val\_k_{j\ i=j=a,b,c})$ 即驗證子、通訊碼及代理密鑰後，自主利用所屬使用者或管理者之公鑰，代理驗證另二方的身份是否合法及訊息是否遭到竄改，若驗證失敗，則將訊息丟棄，不執行後續程序。同樣地，任務代理人收到隨機值及資料擷取代理人收到次密鑰後，均自主性檢查是否有三筆資料，若不符合，同前般丟棄訊息，不執行後續程序。

經本研究代理人自主驗證機制，不僅可達到機敏性資訊存取控制，使用者更毋須線上等待回應認證相關訊息，節省時間成本及網路頻寬。

四、實數驗證

假設具資料存取人員(A、B、C…N)均已完成註冊為合法人員，並分散於各遠端；解開資料庫門檻標準，必須由二位具資料存取權限人員同意，方能執行。若 A 欲存取機密性資料庫，並已經徵求 B、C 同意，彼此約定通訊碼為 2，系統設定 p 值為 13，其原根為 6，認證方程式為 $h(x)=2x^2+8x+5 \bmod 13$，驗證方私鑰 x_{au}=5，公鑰 y_{au}=2。

4.1 接收代理人解密

使用者 A 及管理者 B、C 參數值及說明表如表 4~表 6。

表 4. 使用者 A 參數表

參數	x_a	y_a	t_a	val_k_a	w_a	r_a	c_a	e_a
參數值	3	8	11	5	11	2	10	7
屬性	私鑰	公鑰	隨機值	代理密鑰	驗證子	隨機值	加密值	加密值

表 5. 管理者 B 參數表

參數	x_b	y_b	t_b	val_k_b	w_b	r_b	c_b	e_b
參數值	9	5	5	11	2	3	8	10
屬性	私鑰	公鑰	隨機值	代理密鑰	驗證子	隨機值	加密值	加密值

表 6. 管理者 C 參數表

參數	x_c	y_c	t_c	val_k_c	w_c	r_c	c_c	e_c
參數值	5	2	7	5	7	4	9	8
屬性	私鑰	公鑰	隨機值	代理密鑰	驗證子	隨機值	加密值	加密值

當接收代理人收到訊息 $(w_i,n,c_i,c_{j,i=j=a,b,c})$，針對 c_a 及 e_a 其解密運算結果如下：

使用者 A：

$$C_a=(10)^5=(6^2)^5=(6^5)^2=2^2 \bmod 13$$

$$4*y_{au}^{-r_a}=1 \bmod 13 \quad , \quad y_{au}^{-r_a}=10$$

$$e_a(y_{au}^{\ y_a})^{-1}=7*10 \bmod 13=5=val\_k_a$$

管理者 B：

$$C_b=(8)^5=(6^3)^5=(6^5)^3=8 \bmod 13$$

$$8*y_{au}^{-r_b}=1 \bmod 13 \quad , \quad y_{au}^{-r_b}=5$$

$$e_b(y_{au}^{\ r_a})^{-1}=10*5 \bmod 13=11=val\_k_b$$

管理者 C：

$$Cc=(9)^5=(6^4)^5=(6^5)^4=3 \bmod 13$$

$$3*y_{au}^{-r_c}=1 \bmod 13 \quad , \quad y_{au}^{-r_c}=9$$

$$e_c(y_{au}^{\ r_c})^{-1}=8*9 \bmod 13=7=val\_k_c$$

4.2 各代理人驗證

各代理人代理使用者或管理者互相檢驗合法性，驗證結果如下：

代理人 A：

$$6^{(16)}=2*7*5^2*2^2 \bmod 13$$

$$=9=2*7*5^2*1^2 \bmod 13$$

$=9=9 \bmod 13$

※ 管理者Ｂ、Ｃ確為用本身私鑰簽署代理密鑰之合法人員。

代理人Ｂ：

$6^{(10)}=11*7*8^2*2^2 \bmod 13$

$=4=11*7*8^2*2^2 \bmod 13$

$=4=4 \bmod 13$

※ 使用者Ａ、管理者Ｃ確為用本身私鑰簽署代理密鑰之合法人員。

代理人Ｃ：

$6^{(16)}=11*2*8^2*5^2 \bmod 13$

$=9=11*2*8^2*5^2 \bmod 13$

$=9=9 \bmod 13$

※ 使用者Ａ、管理者Ｂ確為用本身私鑰簽署代理密鑰之合法人員。

4.3 任務代理人驗證

當各代理人驗證成功後，分別產生隨機值給任務代理人， 隨機值如表 7：

表 7. 各代理人產生隨機值

代理人	代理人 A	代理人 B	代理人 C
隨機值	6	7	9

當任務代理人收到隨機值 $I_{i\ i=a,b,c}$，先檢查筆數是否有三筆，若不符合，則表示代理人驗證非全數通過，故不採取後續程序；若相符，則將隨機值代入函數 $h(x)=2x^2+8x+5 \bmod 13$，依序將 I_i 轉換成次密鑰，如表 8：

表 8. 任務代理人產生次密鑰

	A 隨機值	B 隨機值	C 隨機值
	6	7	9
h(x)	$2x^2+8x+5 \bmod 13$		
次密鑰	8	3	5

4.4 任務代理人驗證

資料擷取代理人先檢查隨機值、次密鑰是否有三筆，若不符合，則不執行後續程序，若相符，則將次密鑰結合如下：

$$h_1(x)=8\frac{(x-7)(x-9)}{(6-7)(6-9)}+3\frac{(x-6)(x-9)}{(7-6)(7-9)}+5\frac{(x-6)(x-7)}{(9-6)(9-7)} \bmod 13$$

$=15x^2-18x+31 \bmod 13$

$=2x^2+8x+5 \bmod 13$

資料擷取代理人再將 $h_1(x)$ 與 $h(x)$ 比較，結果如下：

$h_1(x)=2x^2+8x+5 \bmod 13=h(x)$

經比對後相符，資料擷取代理人則開啟資料庫。

五、研究分析及相關研究比較

5.1 安全性分析

Austin[11]提出「密碼學安全性服務」，須包含傳送過程保密性、訊息確認性、完整性及不可否認性。依據該理論，就本研究所達到安全功能及存取控制分析如下：

5.1.1 完整性與保密性

使用者及管理者皆以隨機值 r_i 與驗證方公鑰 y_{au} 加密驗證鑰匙 val_k_i，故傳輸過程中，攻擊者欲從 c_i 推導 r_i，將面臨解離散對數困難；若從 e_i 推導，在無法得知 r_i 情況下，亦無法得知 val_k_i；驗證子 w_i，雖未經加密保護，然欲從 w_i 得知 t_i，攻擊者亦將面臨解離散對數困難，若 w_i 遭到竄改，各代理人驗證時(19)~(21)，將會發現不符情況，而放棄執行後續程序。

5.1.2 確認性

若攻擊者竄改 e_i，將導致使用者及管理者代理密鑰與原產生密驗值不符，使用者或管理者所屬代理人驗證彼此代理祕鑰，將發現錯誤，而不執行後續程序，此外，透過公鑰能相互確認對方身份，避免遭非合法或合法人員冒名攻擊。

5.1.3 不可否認性

由於使用者及管理者所產生代理鑰匙，皆動用本身私鑰簽署，驗證方能透過公鑰驗證，故無法事後否認交易行為。

5.1.4 存取控制

本研究針對機密資訊存取，提出門檻限制，使用者雖具存取機密資訊權限，但須達一

定門檻值人數同意，方能存取機密資訊，此外，本研究驗證伺服器能利用使用者及管理者產生之驗證訊息，可偵測出未授權者之活動及存取。

5.2 效率分析

5.2.1 非同步化驗證處理

本研究利用代理人的特性，實現非同步化驗證處理功能，使用者及管理者僅須將驗證參數交付驗證伺服器，並藉驗證伺服器間代理人相互合作達成訊息與身份確認；就使用者而言，毋須全程線上等待回應，便能達到機密資訊資料存取授權，除可節省時間成本，同時也簡化驗證流程，避免浪費網路頻寬。

5.2.2 代理人集中化管理

本研究採取集中化方式管理代理人，省卻分散式溝通障礙與麻煩，藉以避免因網路壅塞，而降低整體效能。

5.3 相關研究比較

本研究藉由代理人特性實行非對稱式密碼及門檻方法，提出具離線(非同步化)身份認證及別於傳統單一密鑰之認證方式，藉以改善認證效能及單一密鑰遭竊取之風險，茲將本研究與 Hwang 等學者，提出基於 RSA 密碼系統之門檻式代理簽章方法，就 Wang[12]等學者提出的安全性分析比較如下：

5.3.1 私密性

(1)Hwang 等學者

若門檻值以上之所有代理簽章者共謀，可得到代理簽章鑰匙 D。原始簽章者私鑰，具有被代理簽章者揭露之風險。

(2)本研究

本研究採用驗證伺服器對使用者及管理者身份驗證，使用者及管理者僅須將代理密鑰及相關參數傳送至驗證伺服器，即可完成資料存取(授權)，若驗證方惡意欲從代理密鑰推導使用者及管理者密鑰，理論上將不可行，因代理密鑰利用隨機值 t_i 結合私鑰；因 t_i 無法得知情況下，驗證方將面臨解離散對數困難。

5.3.2 代理簽章防護

(1)Hwang 等學者

所有代理簽署鑰匙 $k_{i,i=1\sim n}$ 、群體代理簽章鑰匙 D 及代理簽章驗證鑰匙 E，均由原始簽章者產生，故可任意產生訊息，透過直接運算代理簽章 S，並交給驗證者；驗證者僅檢查是否符合，並未檢查各代理簽章者是否動用過自己的私鑰，故原始簽章可偽造群體簽章過的訊息。

(2)本研究

本研究代理密鑰均由使用者及管理者單獨產生，並於進行資料存取前，使用者與管理者間協調共同交易通訊碼，於密鑰無法得知情況下，任何人均無法進行偽造代理密鑰。

5.3.3 不可否認性及確認簽章者

(1)Hwang 等學者

代理簽章匯整者(Combiner)並未擁有原始簽章者及代理簽章者簽章記錄，故原始簽章者及代理簽章者能夠事後否認簽章事實。

(2)本研究

本研究之代理密鑰均須動用密鑰簽署，交到驗證伺服器後，其屬代理人，依(19)~(21)代為驗證彼此身份，若結果相符，可確認為合法使用者或管理者，否則即為非合法人員或合法人員偽造訊息，系統便不執行後續程序。此外，因代理密鑰均動用過私鑰簽署，故使用者及管理者無法事後否認交易事實。

5.3.4 不可偽造性

(1) Hwang 等學者

基於 E、e_0 及 m_w 是公開值，故外部非法人員藉由 $e_0{}^{m_w} - E$ 得知其值為 $\phi(N_0)$ 的倍數，並分解原始簽章者之模 N_0 ，進而推導其私鑰，便可執行偽造攻擊。

(2)本研究

本研究代理密鑰由驗證方公鑰加密，若遭外部惡意者竊取，在無法得知驗證方私鑰，將面臨解離散對數困難。若竄改 e_i 、 w_i 等驗證參數，各代理人驗證時(19)~(21)，將會發現不符情況，而放棄執行後續程序。故外部攻擊者無法藉由竊取參數，進行偽造攻擊。

六、結論

本研究主要針對機密性資料存取，提出安全管理方法，透過實數驗算及安全、效率分析，證實本研究之可行性，以下就本研究未來要發展方向提出說明：

1、門檻值最佳化

基於門檻值限制，欲開啟資料庫，須得到門檻值以上人員同意(本研究設定為 3 員)，若門檻值太高雖然比較安全，但代理人相互間驗證次數 n(n-1)及次密鑰還原亦隨之變多，影響驗證效率，故如何精確取決門檻值，兼顧安全及效率，便是很重要課題。

2、隨機數無法重覆使用

本研究為降低系統負荷，利用數位簽署方法取代加解密運算；若使用者須再存取機密資訊，則使用者及門檻成員必須產生新的隨機數，否則攻擊者只要竊取同樣訊息驗證值及驗證參數，必定可利用聯立方程式推導出使用者私鑰。

本研究針對機密資訊存取提出一套方法論，基於所有學術研究最後目標就是應用於實作，故未來本研究將朝理論實現，使理論機制成為可實行之應用系統。

參考文獻

[1] Briney, A.,“Security Focused Survey 2000” Information Security Magazine, pp.40-68, September, 2000.

[2] Wang, H. and Wang, C., “Intelligent Agents in the Nuclear Industry”, Computer, Vol. 30, pp. 28-31, Nov. 1997.

[3] 郭木興，電子商務理論與技術，碁峰資訊股份有限公司，2001。

[4] Ferber, J., “Multi-Agent Systems”, An Introduction to Distributed Artificial Intelligence. Addison-Wesley Pub Co, 1999.

[5] Shakshuki, E., Luo, Z., and Gong, J., “An agent-based approach to security service”,Journal of Network and Computer Application, Vol.28 , pp. 183-208,2005.

[6] Lin, I. C., Ou, H. H., and Hwang,M.S., “Efficient access control and key management schemes for mobile agents”, Computer Standards & Interfaces ,Vol.26 , No.5,pp.423-433,2004.

[7] Shamir, A., “How to share a secret”, Communications of the ACM, Vol. 22, No. 11, pp.612-613, 1979.

[8] Blakley, G.. R., “Safeguarding Cryptographic Keys”, Proceedings AFIPS 1979 National Computer Conference, Vol. 48, pp. 313-317, 1979.

[9] Hwang, M. S., Lu, J. L., and Lin, I. C., “A Practical (t,n) Threshold Proxy Signature Scheme Based on the RSA Cryptosystem”, IEEE Transaction on Knowledge and Data Engineering, Vol.15, No 6, pp.1552-1560, 2003.

[10] Wang, G.., Bao, F., Zhou, J., and Deng , R. H., “Comments on a Threshold Proxy Signature Scheme Based on the RSA Cryptosystem”,IEEE Transaction on Knowledge and Data Engineering,,Vol.15, No. 10,pp.1309-1311,2004.

[11] Austin, T., “PKI：A Wiley Tech Brief”, John Wily& Sons,New York , 2000.