

動態存取控制之雲端服務設計－以空軍航管模擬訓練系統為例

蘇品長¹ 陳營和² 張嘉烈¹ 葉昱宗¹ 曾健豪¹

¹ 國防大學資訊管理學系

² 空軍通信航管資訊聯隊

論文編號：3601-10

收稿 2014 年 03 月 12 日 → 第一次修訂 2014 年 04 月 21 日 → 同意刊登 2015 年 08 月 07 日

摘要

國防部規劃在人力裁減狀況下，能藉由建置雲端環境有效率的執行任務，以改善資源佈署、資安防護等問題，以利任務順遂。然而，雲端運算仍存在著一些安全上的疑慮，以現今觀點來看，空軍刻正建置飛航管制模擬訓練系統，其中航管人員依屬性不同，區分了不同的席位，區分不同等級，也賦予不同的任務，每個人需要的控制權限也不相同。因此，存取權限的管理及異動需要仰賴後端龐大的資料庫，易衍生出浪費記憶體空間及冗餘時間等問題。本研究提出建置一個適切的雲端環境應用於空軍飛航管制訓練系統，運用橢圓曲線加密及自我認證等機制，加上動態存取控制，增加航行管制人員訓練服務，在降低管理開銷，不浪費後端資料庫條件下，讓使用者在特定權限內安全的存取資料，且不需考量到資安問題，符合部隊建軍備戰需求。

關鍵詞：雲端服務運算、飛航管制模擬訓練、動態存取控制

Design Dynamic Data Access Control Schemes for Cloud Service — A Case on Air Traffic Control Training System

**Pin-Chang Su¹ Ying-Ho Chen² Chia-Lieh Chang¹
¹Yui-Chang Yeh Jian-Hao Zeng¹**

¹Department of Information Management, National Defense University, Taiwan, R.O.C.

²Air Force News Wing ATC Communications, Taiwan, R.O.C.

Abstract

The National Defense Department is planning to construct a “cloud environment” in order to execute missions efficiently; hence, fixing problems such as resources allocation and information security while minimizing human resources. However, cloud computing still consists some questions regarding on the safety issue. From the perspective nowadays, the air force is currently constructing an air traffic control training simulator system, and each operator is assigned with different position, level, and mission due to various job attributes. Thus, an enormous data base is needed for the management of various access authorizations. Such action can cause waste in memory space and time easily. This research will provide an appropriate “cloud environment” that is suitable for air force’s air traffic control training simulator system through elliptical curve cryptography and self-certified certificate along with remote access control. This research is suitable for increasing the amount of training for the air traffic controller and decreasing management cost without causing waste for the data base, and provides the users with the necessary information under particular authorization without worries for information security. Hence, the mechanism designed in this study meets the requirements of the troop’s armed preparation.

Keywords: Cloud Services, Air Traffic Control Simulation & Training System, Dynamic Access Control

壹、前言

美國的國防部於2012年7月發表其雲端策略指出其目標是建立一聯合資訊環境。反觀我國行政院在2010年4月29日第3193次院會核定通過的「雲端運算產業發展方案」，期望實現「邁向科技強國-藉雲端運算升級台灣成為資訊應用與技術先進國家」之發展願景。國防部通次室也於2010年5月6日頒布「國軍雲端服務規劃指導計畫」，復於2011年3月31日頒布「國軍雲端服務發展計畫」，直接指出國軍雲端服務之近、中、遠程的發展目標(詹子銘，2013)。

國軍雲端目前已依「國軍雲端服務發展計畫」逐步規劃建置，而組織規劃資訊安全管理的策略要求中，經常會提到人員(People)、流程(Process)、技術(Technology)，俗稱為「PPT」的思考架構，雲端運算的存取控制管理仍是目前必須注意的安全議題，尤其依照業務屬性訂立安全的作業流程與記錄，防禦可能來自內部與外部的各項威脅等。思考如何確保資訊只讓授權的人員存取是否以文件化方式建立了各項和資訊及存取有關的政策。至於在技術方面，針對網路、作業系統與應用系統，是否劃分了安全邊界、良好的使用者身分識別，並且賦予適當的連線控制(Net Admin 網管人，2012)。

國軍中又以空軍負有捍衛我國領空權的職責，空軍訓練為國軍建軍備戰之基礎，目前刻正規劃建置飛航管制模擬訓練系統。構想為將飛行員不定期自台灣各機場集中訓練，但恐因種種因素而降低了使用率。若能建置一套雲端環境，提供訓練服務，便可降低集中訓練的開銷，增加效率，提升訓練品質。

然而就傳統存取控制方法的觀點來看，存取權限的管理仍需要仰賴後端龐大的資料庫，易衍生浪費龐大的記憶體空間及權限異動造成等問題。因此一套完善的雲端運算環境，必須考量後端存取控制的安全性與適切性，存取權限及金鑰管理等皆需大量仰賴後端的安全管理機制及資料庫的儲存空間。

本研究藉由橢圓曲線加密及自我認證等機制，設計出適用於空軍飛航管制訓練系統之動態存取控制，以提供航行管制人員隨需的使用訓練服務，在不增減後端龐大資料庫情況下，讓使用者在特定的權限內安全的存取資料，並確保資料安全。讓使用者在特定的權限內安全的存取資料，達到實際需求將是本研究的研究及探討重點。

本論文架構一共分為五章，各章說明如下：第一章：說明研究背景、動機與研究目的；第二章為文獻探討，簡單介紹與本論文相關研究，第三章為研究方法，第四章為安全性及效益分析，第五章為結論及未來研究方向。

貳、文獻探討

本章架構一共分為三節，說明如下：第一節：介紹飛航管制模擬訓練系統；第二節為雲端運算技術簡介，第三段為本論文密碼學相關知識。

一、飛航管制模擬訓練系統

提供航行管制人員執行模擬訓練，目標為建置高效能、高逼真度、低成本、易維護之訓練系統。施訓對象為空軍各機場管制塔台與地面進場管制台(Ground Control Approach, GCA)飛航管制人員，模擬接近實際環境，結合各項任務環境，提升航管人員能力與經驗，區分為飛航管制模擬訓練系統架構、飛航管制塔台模擬訓練及 GCA 導引訓練三部分。茲就系統概述如後：

(一)飛航管制模擬訓練系統架構

「飛航管制模擬訓練系統」全系統架構共計分為主計算機分系統、視效分系統、音效通訊分系統、輸出入介面分系統、控制艙台分系統等五大分系統，如圖1。

飛航管制模擬訓練系統架構圖

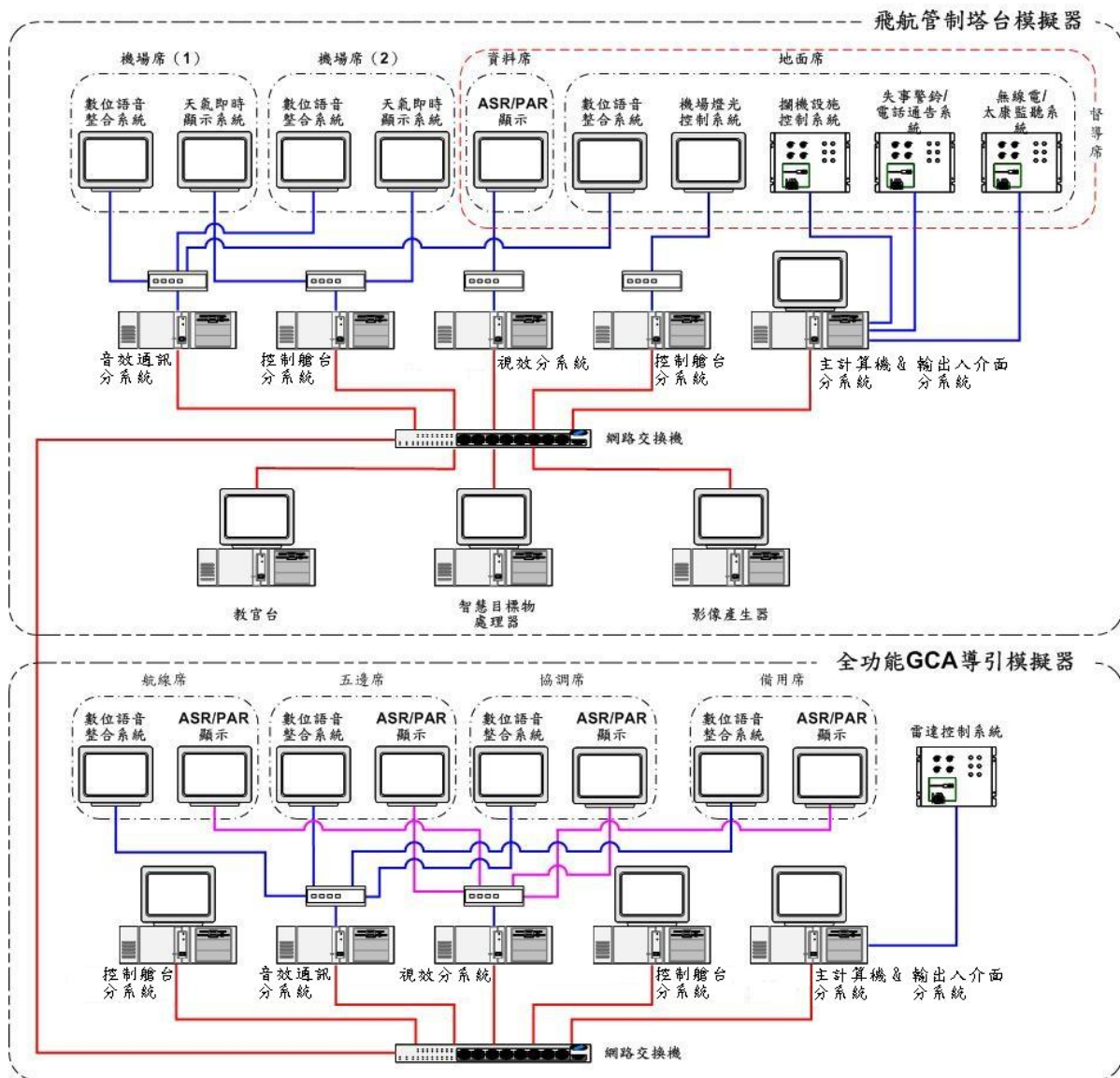


圖 1 飛航管制模擬訓練系統架構圖

(二) 飛航管制塔台模擬訓練

依訓練功能區分塔台管制模擬訓練及 GCA 導引模擬訓練；塔台管制訓練係依空軍塔台任務需求建置飛航管制塔台模擬器，此模擬器可提供 360 度全塔瞭望視窗、機場燈光控制、天氣即時顯示、飛行管理系統、GCA 顯示、塔台管制操控台顯示及各式有關航管、飛安及緊急情況等場景，以訓練機場管制塔台內相關管制人員(包括機場管制席、地面管制席、資料席與督導席等席位)之近、遠端管制技

能、裝備操作、緊急狀況判斷與應變能力。

(三) GCA 導引訓練

依空軍助航雷達系統建置全功能 GCA 導引模擬器，此模擬器可提供航線席、最後進場席、督導席等席位，用以引導航機所需之雷達初、次級訊號、視頻地圖等功能，觸控式通信系統顯示與操作功能，遂行進場管制、一般管制、特殊與緊急狀況處置等訓練。

然而，因應未來桃園國際機場航

空城及松山機場的擴建，該處營區未來將面臨搬遷，而該系統係屬單機方式運作且仰賴後端龐大的資料庫存放大量的用戶權限資料，易衍生浪費龐大的記憶體空間或是權限異動造成管理上負擔及時間的浪費等問題。

二、雲端運算

維基百科則認為：雲端運算是種能夠將動態伸縮的虛擬化資源，透過網路以服務的方式提供給使用者的運算模式，使用者不需要知道如何管理那些支援運算的基礎設施(維基百科，2012)。雲端運算的架構，須具備五種特性，包括了「抽象化的

基礎設施」、「資源的自由化」、「服務導向的架構」、「動態的資源調配」以及「新型消費與分配」，透過網路連結以提供服務，使用者只需要在意是否能夠順利的取得所需要的網路服務資源，不需要考慮需要的應用服務支援的資源是否充足，雲端運算是一種基於網際網路的新運算架構，而雲端服務即是在此架構下的產物，目前雲端服務已逐漸普及於許多應用領域上，強大且彈性付費的運算與儲存能力吸引了許多新型網路服務採用(蔡一郎，2010)。各雲端運算定義研究如表 1。

表 1 雲端運算的定義

雲端運算	
來源	特色
National Institute of Standard and Technology(NIST)	具備大規模電腦叢集(Clusters)，虛擬化的軟體/伺服器的框架，與在此框架上運作的應用系統組合的架構，提供用戶可擴充的公用計算能力，為應用軟體服務提供彈性調整伺服器資源或代管各種應用系統。
Gartner Group	具備大量且可擴充的 IT 相關能力的運算方式，透過網際網路技術，並以服務的形式，提供給外部使用者。
Wikipedia	是一種基於網際網路的運算方式，透過這種方式，共享的軟硬體資源和訊息可以按需求提供給電腦和其他裝置。
Forrester	即時的 IT 能力運算網路平台，透過網際網路，被請求、供應、傳遞、以及消費。
IDC	高度具有彈性及延展性的運算中心，可以提供使用者所需程式，依據資源使用多寡來收費
Google	應用程式和資料在雲端，可以透過任何裝置存取，使用瀏覽器在網雲間相互連通。
Microsoft	由微軟資料中心供應的網路雲端服務平台，可提供一套作業系統和一組程式開發者服務，可供個人或群體操作。
IBM	分享網路資訊服務的模式，使用者看到的只有服務本身，不用關心相關基礎的建置。

三、密碼學技術應用

本節將與本研究相關密碼技術做一個整理，共分為橢圓曲線公開金鑰密碼系統、隨機背包密碼系統及自我認證公開金鑰密碼系統三部分，概述如後：

(一)橢圓曲線公開金鑰密碼系統

自從 Miller(1985)與 Koblitz(1987)兩位學者分別提出利用橢圓曲線來實作公開金鑰密碼系統，發展出一套能提供與 RSA(Rivest, Shamir and Adleman)及 ELGamal 非對稱式金鑰密碼系統相同安全強度且所需要金鑰長度卻較短的橢圓曲線密碼系統。其橢圓曲線一般方程式為：

$y^2 + axy + by = x^3 + cx^2 + dx + e$ 其中 a 、 b 、 c 、 d 、 e 是實數。在橢圓曲線中，點加法運算是經過特別定義的，除此之外，也另外定義一個無窮遠點 O ，對任一點 $A \in E$ ， $A + O = O + A = A$ 。

橢圓曲線定義(肖攸安，2006)：令 p 是大於 3 的質數，在 $GF(p)$ 中的橢圓曲線 $E: y^2 = x^3 + ax + b \pmod{p}$

，其中 $4a^3 + 27b^2 \neq 0 \pmod{p}$ 。而此橢圓曲線群 $GF(p)$ 中的點加法運算定義為如下：令 $A = (x_1, y_1)$ 與 $B = (x_2, y_2)$ 為 E 上的點，則若 $x_2 = x_1$ 且 $y_2 = -y_1$ ，則 $A + B = O$ ；否則 $A + B = (x_3, y_3)$ ，其中

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1。$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } A \neq B \\ \frac{3x_1^2 + a}{2y_1} & \text{if } A = B \end{cases}$$

橢圓曲線密碼系統的另一個優點是其加密的密鑰長度短，在同樣的安全度之下，橢圓曲線密碼系統僅需要較小的密鑰長度，相同地，在同樣的密鑰長度下，橢圓曲線密碼系統卻擁有更高的安全性。

(二)隨機背包密碼系統

假設我們有一個背包能裝載的物品重量是固定的，同時我們也有非常多的物品，而每個物品的重量都不一

定相同，那如何能找到一堆物品其總重量剛好符合背包所能裝載的重量即是所謂的背包難題。它的數學描述是給定一個自然數數列 $B = \{b_1, b_2, \dots, b_n\}$ 及一數 S ，是否存在一子數列 $B' \subseteq B$ ，其中 $B' = \{b'_1, b'_2, \dots, b'_m\}$ $PPD = \{W_0, u_0\}$ ，使得 $\sum_{i=1}^m b'_i = S$ ？

自從 1976 年 Diffie 及 Hellman(1976)向世人介紹了公開金鑰密碼的概念之後，其中較著名的為 1976 年 Merkle-Hellman 背包密碼系統(Merkle and Hellman, 1978)。背包難題經證實為一個 NP-Complete 的問題，無法在多項式時間內解決，基於背包難題所設計的密碼系統最大優點為加解密(或簽署驗證)速度相當快，故將其套用在密碼系統的設計上有其優點。

但是這種密碼系統中其「超增序列(Super-Increasing Sequence)」被許多學者發現其弱點並對此展開攻擊，第一位成功攻擊 Merkle-Hellman 背包密碼系統的學者是 Shamir(1984)，並且陸續又被許多學者提出攻擊的方式，其中以 Brickell(1984)的學者所提出的攻擊方式較為特別，它的攻擊方式稱為低密度攻擊，主要是背包密碼系統中的超增序列數值，在整個數列中所佔的密度太低，因此就有可能被猜出來，導致背包密碼系統因此瓦解。

背包密碼系統設計時大多以易解背包難題方式設計序列，然後再偽裝成看似困難的背包難題，但事實上仍屬於易解背包難題，容易面臨低密度攻擊的問題，是肇致系統不安全的原因；另外，如果對易解背包難題偽裝不充分，則容易受到密鑰恢復攻擊，因此，王保倉等人(2010)提出「基於隨機背包的公鑰密碼」，植基於隨機選取的背包難題，而非人為建構的易解背包難題，且該演算法僅以簡單的加法及模數運算即可完成加解密運作，運算速度快，並證明該方法可以抵抗所有直接求解背包難題而發起的攻擊

及密鑰恢復攻擊。

「基于隨機背包的公鑰密碼」概分三階段，分別為密鑰生成、加密及解密階段：

1. 密鑰生成階段

隨機選取 n 維向量 $U = (u_1, u_2, \dots, u_n)$ ，且 u_i 均為正整數。計算向量 $V = (v_1, v_2, \dots, v_n)$ ， $v_i = u_i - 2^{n-1}, i = 1, \dots, n$ 。隨機選取兩個質數 g 和 f ，使得 g 大於向量 U 的總和， f 大於兩倍向量 V 正負差之總和。

$$g > \sum_{i=1}^n u_i, f > 2\max\left\{\sum_{v_i>0} v_i, -\sum_{v_i<0} v_i\right\}$$

利用中國餘式定理計算公鑰

$$A = (a_1, a_2, \dots, a_n), 0 \leq a_i \leq gf - 1$$

$$a_i \equiv u_i \pmod{g}, a_i \equiv v_i \pmod{f},$$

$$i = 1, \dots, n$$

2. 加密階段

將訊息 m 換算為 n 維二進位 $(m)_2 = m_1, m_2, \dots, m_n$ ，其中 $m_i \in [0, 1]$ 。將訊息 $(m)_2 = m_1, m_2, \dots, m_n$ 與公鑰 $A = (a_1, a_2, \dots, a_n)$ 加密。

$$c = a_1 m_1 + a_2 m_2 + \dots, a_n m_n$$

3. 解密階段

收到密文 C 後，透過下列計算即可得到訊息 m 。

$$c_g = c \bmod g, 0 \leq c_g < g - 1$$

$$c_f = c \bmod f, -\frac{c_f}{2} < c_f \leq \frac{c_f}{2}$$

$$(c_g - c_f)_2 = (m)_2 = (m_1, m_2, \dots, m_n)$$

m_1 為二進位的最高位元， m_n 則為二進位的最低位元。

(三) 自我認證公開金鑰密碼系統

自我認證機制之目的在於授權階段可由使用者參與公鑰的計算，而使用階段可以獨立進行身分自我認證，

不需再透過公證第三方的身分認證的演算法。自我認證機制不但可以避免一般憑證授權中心 (Certification Authority, CA) 製發憑證的過程中，因憑證授權中心代替用戶選定私鑰，而會有憑證中心偽冒使用者身分的能力的隱憂；同時可以降低整體認證系統在公鑰儲存、計算與管理的成本與風險。

Girault(1991)運用 RSA 系統所設計的自我驗證密碼系統，共包含系統建置、使用者註冊及身分識別等三個階段，各階段分述如下(如圖 2)：

1. 系統建置階段

認證中心以 RSA 的方式取得 e ， d 與 N ，其中 e 為系統中心的公鑰； d 為私鑰，參數敘述如下：

p, q ：選擇兩個大質數。

N ：為 p 與 q 的相乘積之合成數。

$$N = p \times q$$

e ：認證中心的公鑰。

$$\text{GCD}(e, (p-1)(q-1)) = 1$$

d ：認證中心的私鑰。

$$ed = 1 \bmod (p-1)(q-1)$$

g ：在乘法群 Z_N^* 中最大序的整數。

系統中心公開 $\{N, e, h()\}$ ，秘密保留 d ，而其中 p 與 q 可在計算完 d 後丟棄。

2. 使用者註冊階段

使用者 U_A 自行選定自己的私鑰 S_A ，並計算出 $V_A = g^{-S_A} \pmod{N}$ 後，再將身分識別碼 ID_A 與 V_A 傳給系統認證中心。

系統認證中心計算使用者 U_A 的公鑰 P_A ， $P_A = (V_A - ID_A)^d \pmod{N}$ ，並將 P_A 傳回使用者 U_A ，使用者 U_A 驗證 $P_A^e + ID_A = V_A$ ，因 $(V_A^d - ID_A^d)^e + ID_A = V_A$ ，若成立則使用者 U_A 的公鑰為 P_A ，私鑰為 S_A 。

3. 身分識別階段

當使用者 U_A 和 U_B 兩人相互通訊

時，他們之間的身分確認如下：

- (1) 使用者 U_A 將其 ID_A 和 P_A 傳給使用者 U_B ，然後使用者 U_B 計算：
 $V_A = (P_A^e + ID_A)(\text{mod } N)$ 使用者 U_A 選擇一個隨機參數值 x ，計算 $t = g^x(\text{mod } N)$ 後，將 t 傳送給使用者 U_B 。
- (2) 使用者 U_B 選擇一個隨機參數值 C ，並將其傳給使用者 U_A 。使用者 U_A 計算 $y = x + S_A \times$

$C(\text{mod } N)$ 後，並將 y 傳送給使用者 U_B 。最後使用者 U_B 利用驗證式：

$$g^y \times V_A^C = t(\text{mod } N)$$

$$g^{x+S_A C} \times g^{-S_A C} = g^x(\text{mod } N)$$

若等式成立則可證明使用者 U_A 的身分；同理，使用者 U_A 也可以此方式驗證 U_B 的身分。

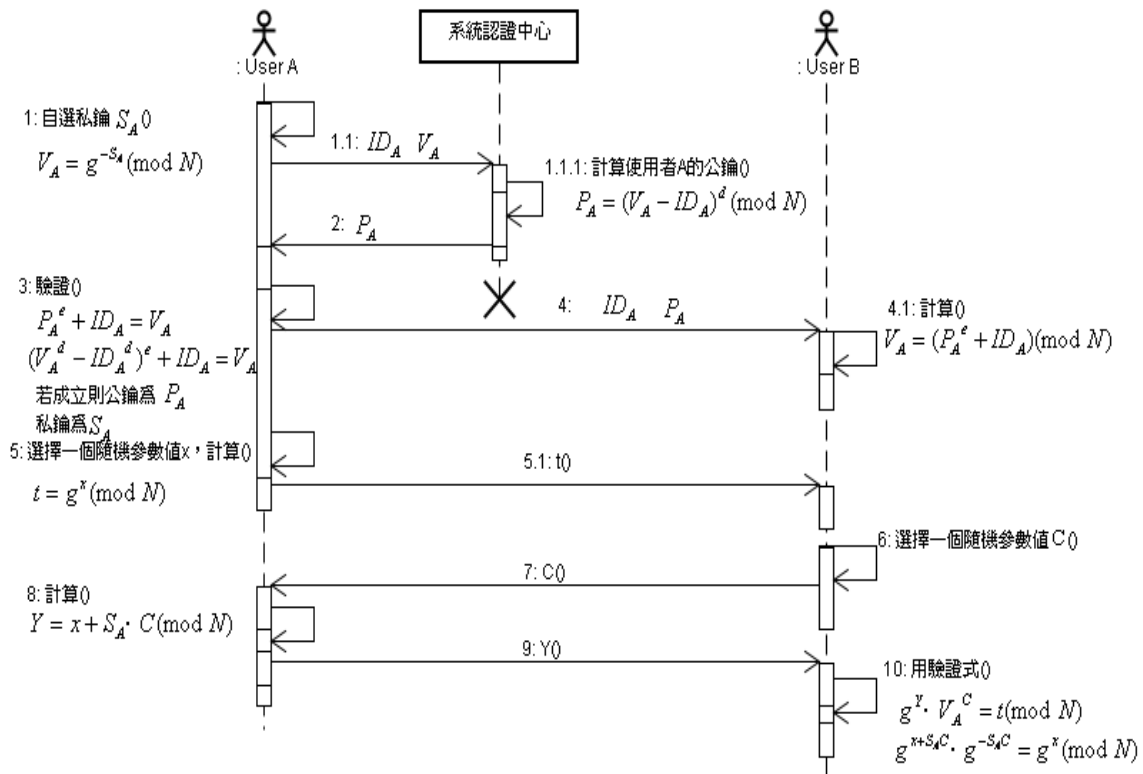


圖 2 Girault 自我認證階段循序圖

(四)動態存取控制設計雲端環境

國軍網路現採實體隔離方式施行，並依國防部頒定之「國軍雲端服務發展計畫」執行規劃並逐步建置國軍雲端服務，而為及早建置一個適合飛航管制模擬訓練系統的雲端環境，本研究將針對存取控制以取得雲端服務為本研究之設計研究之重點。因此，我們將飛航管制模擬訓練系統視為一雲

端服務中心，各飛航管制人員為使用者(含民航局飛航管制人員)，使用者可以在任何地點透過網路連線到雲端服務中心，並依照需求使用雲端服務，並且有一第三方之認證中心負責提供註冊單位之金鑰，任一使用者均需向認證中心申請註冊，以利雲端服務中心驗證使用者並依權限提供服務，設計初步構想，如圖 3。

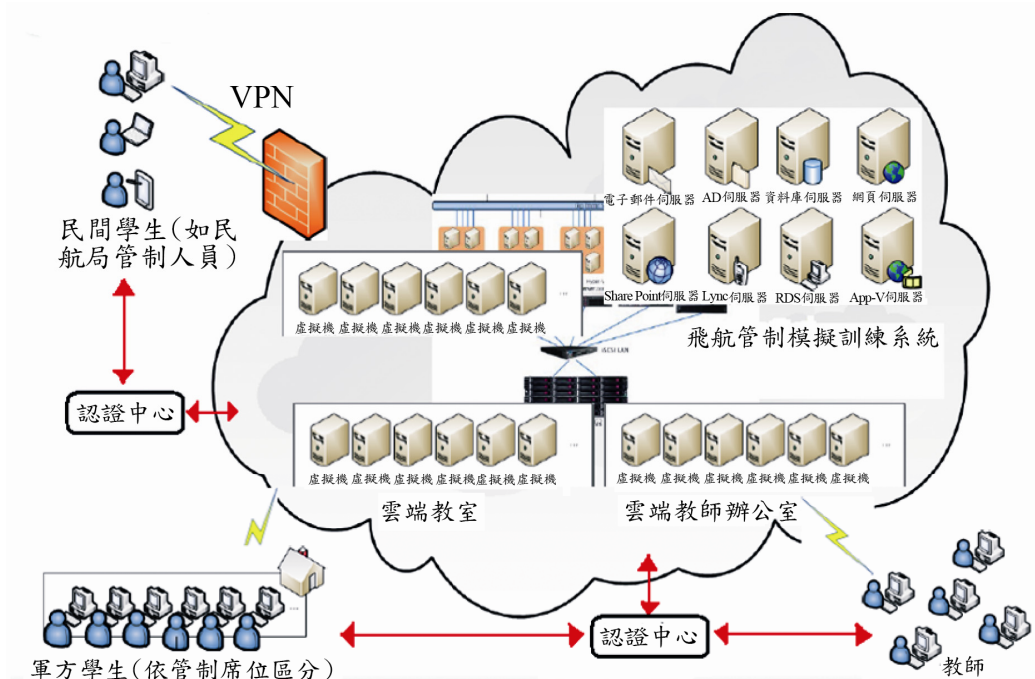


圖 3 系統示意圖

叁、研究方法

本章設計的系統演算法共分成八個階段，分別為系統參數符號說明、系統初始階段、廠商與採購中心相互驗證階段、訊息盲化階段、簽章階段、採購中心與採購機關相互驗證階段、解盲簽章階段、驗證階段，各階段的詳細作法描述如下：本系統區分為系統初始、登入註冊、驗證及服務存取等四階段。系統初始階段由驗證中心公開相關參數，服務中心建立服務及權限種類序列給驗證中心提供使用者查詢；

登入階段是使用者與服務中心向驗證中心註冊；驗證階段是使用者及服務中心與驗證中心相互驗證是否為合法身分並建立公享密鑰；服務存取階段是使用者將授權服務及存取權限值加密後傳送服中心請求服務使用，服務中心解密後依照授權服務及存取權限值提供服務。

一、系統參數符號說明

系統初始時針對密碼系統作一個參數設定選擇，以下針對本研究中各參數進行說明，如表 2 所示：

表 2 系統使用符號之說明

項次	符號	說明	項次	符號	說明
1	U_A	使用者 A	12	PK_{AC}	驗證中心公鑰
2	W_{Si}	雲端服務中心	13	sk_{AC}	驗證中心私鑰
3	AC	驗證中心	14	PK_A, PK_S	驗證中心產生給 U_A 及 W_{Si} 的驗證公鑰
4	$E(F_q)$	橢圓曲線	15	S_A, S_S	U_A 及 W_{Si} 的公開金鑰
5	A	控管服務之序列	16	sk_A, sk_S	U_A 及 W_{Si} 的私密金鑰
6	t_A	授權服務種類之序列	17	$K_{(A,S)}$	U_A 及 W_{Si} 之共享金鑰
7	B	使用服務權限序列	18	k_A, k'_A	U_A 隨機的一個參數

8	t_B	授權服務權限種類序列	19	$Af、At$	服務使用權限值及存取權限種類值
9	V_A	U_A 的簽名檔	20	$A'f、A't$	使用者自訂之服務使用權限值及存取權限種類值
10	W_A	U_A 的簽章	21	C_{A_0}	含服務使用權限值、存取權限種類值與雙方共享秘鑰的權限密文
11	$d_A、d_S$	U_A 及 W_{S_i} 選取的隨機參數	22	n'	表示與相同一數字 n 同時發生之步驟

二、系統初始階段

系統初始階段含驗證中心建置階段、雲端服務中心(W_{S_i})建置服務及權限序列，如圖 4，分述如後：

(一)驗證中心(AC)建置階段，程序如下：

步驟一：由驗證中心(AC)在有限域 F_q 上選取一條安全的橢圓曲線 q 為一個 160bit 以上之大質數，在 $E(F_q)$ 上選一階數(order)為 n 的基點 G ，使得 $nG = O$ ，其中 O 為此橢圓曲線之無窮遠點。

步驟二：AC 選擇一個單向無碰撞雜湊函數 $h()$ 及私鑰 sk_{AC} ，並計算公開金鑰 PK_{AC}

$$PK_{AC} = sk_{AC}G \quad (1)$$

步驟三：AC 公開 $E(F_q)$ 、 G 、 n 、 $h()$ 。

(二)雲端服務中心(W_{S_i})建置服務及權限序列，程序如下：

步驟一：服務中心依控管之服務種類及數量，建立授權服務序列。

- 隨機選取 n 維向量，且 u_i 均為正整數 $U = (u_1, u_2, \dots, u_n)$ 。
- 計算向量 $V = (v_1, v_2, \dots, v_n)$ ，其

中 $v_i = u_i - 2^{n-1}, i = 1, \dots, n$ 。

- 隨機選取兩個質數 g_n 和 f_n (須滿足 $q > 4g_nf_n + 1$)，使得 g_n 大於向量 U 的總和， f_n 大於兩倍向量 V 加總絕對值之最大值。

$$g > \sum_{i=1}^n u_i, f > 2 \max \{ \sum_{v_i > 0} v_i, -\sum_{v_i < 0} v_i \} \quad (2)$$

- 利用中國餘式定理求得服務序列

$$\begin{aligned} A &= (a_1, a_2, \dots, a_n), \\ 0 &\leq a_i \leq g_nf_n - 1 \\ a_i &\equiv u_i \pmod{g_n}, \\ a_i &\equiv v_i \pmod{f_n}, \\ i &= 1, \dots, n \end{aligned} \quad (3)$$

- 以 $[0,1]$ 分別代表是否允許使用者使用該服務。

$$t_A = (t_1, t_2, \dots, t_n), t_n \in [0,1] \quad (4)$$

- 計算服務使用權限值。

$$Af = \sum_{i=1}^n A \times t_A \quad (5)$$

步驟二：服務中心建立授權之服務存取權限種類序列。

- 隨機選取 m 維向量計算向量

$U^* = (u_1^*, u_2^*, \dots, u_m^*)$ ，且 u_i^* 均為正整數

➤ 計算向量 $V^* = (v_1^*, v_2^*, \dots, v_m^*)$ ，其中 $v_i^* = u_i^* - 2^{m-1}, i = 1, \dots, m$ 。

➤ 隨機選取兩個質數 g_m 和 f_m ，須滿足 $q > 4g_m f_m + 1$ (蘇品長等，2004)，使得 g_m 大於向量 U 的總和， f_m 大於兩倍向量 V 正負差之總和。

➤ $g > \sum_{i=1}^n u_i, f > 2\max\{\sum_{v_i>0} v_i, -\sum_{v_i<0} v_i\}$ (6)

➤ 使用中國餘式定理計算權限種類序列

$$B = (b_1, b_2, \dots, b_n),$$

$$\begin{aligned} 0 &\leq b_i \leq g_m f_m - 1 \\ b_i &\equiv u_i^* (\text{mod } g_m), \\ b_i &\equiv v_i^* (\text{mod } f_m) \quad i = 1, \dots, m \end{aligned} \quad (7)$$

➤ 以 $[0,1]$ 分別代表是否允許使用者使用該服務。

$$t_B = (t_1, t_2, \dots, t_m), t_m \in [0,1] \quad (8)$$

➤ 計算授權服務之存取權限種類值。

$$At = \sum_{i=1}^m B \times t_B \quad (9)$$

步驟三：服務中心將服務序列 A 及存取權限種類序列 B 傳送給 AC ，俾利使用者查詢。

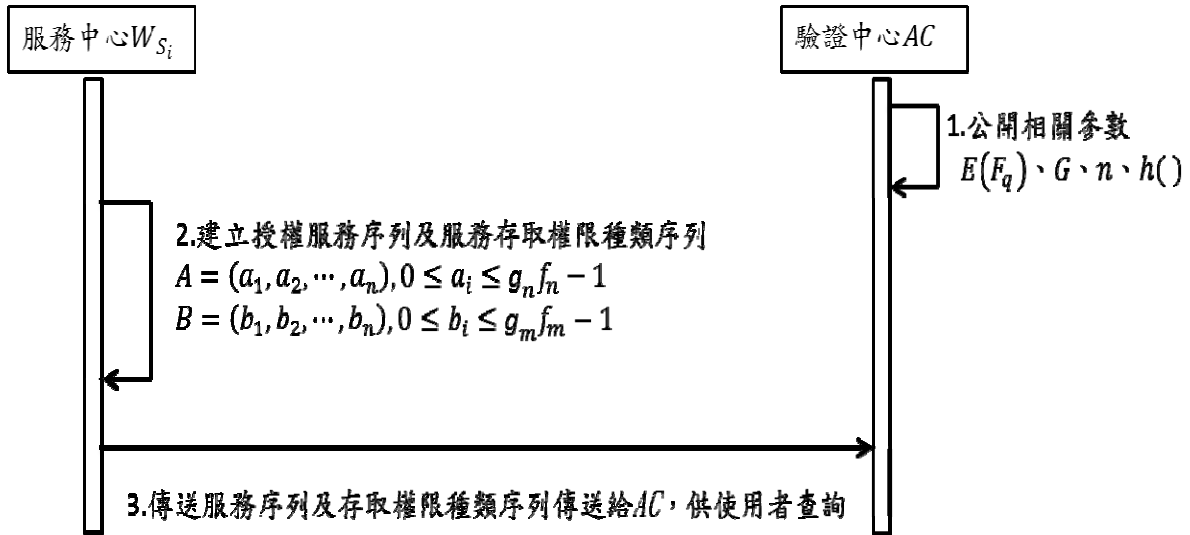


圖 4 初始階段

三、登入註冊階段

在登入階段，使用者 U_A 及服務中心 W_{Si} 向驗證中心註冊，參與金鑰建置，如圖 5。

步驟一：使用者 U_A 以自己 ID_A 及隨機參數 d_A ， $d_A \in [2, n-2]$ ，透過單向無碰撞雜湊函數 $h()$ 產生簽名檔 V_A ，並將 ID_A 與 V_A 與傳給驗證中心。

$$V_A = h(d_A \parallel ID_A)G \quad (10)$$

步驟二：驗證中心(AC)選擇一隨機參數值 $k_A \in [2, n-2]$ 計算 U_A 之驗證公鑰 PK_A 及簽章 W_A 後傳給 U_A ，計算式如下：

$$\begin{aligned} PK_A &= V_A + (k_A - h(ID_A))G \\ &= (q_{ax}, q_{ay}) \end{aligned} \quad (11)$$

$$\begin{aligned} W_A &= \\ &k_A + sk_{AC}(q_{ax} + h(ID_A)) \end{aligned} \quad (12)$$

步驟三： U_A 利用 AC 傳回之參數(W_A 、 PK_A)自己計算私鑰 sk_A ，並利用簽章 W_A 驗證公鑰 PK_A 的正確性，計算式如下：

$$sk_A = [W_A + h(d_A \parallel ID_A)] \quad (13)$$

證明式如下：

$$\because S_A = sk_A G \quad (14)$$

$$S_A = [k_A + sk_{AC}(q_{ax} + h(ID_A)) + h(d_A \parallel ID_A)]G \quad (15)$$

$$\begin{aligned} S_A &= [k_A \\ &+ sk_{AC}(q_{ax} \\ &+ h(ID_A))]G + h(d_A \\ &\parallel ID_A)G \end{aligned} \quad (16)$$

$$\because PK_{AC} = sk_{AC}G \quad (17)$$

$$\begin{aligned} S_A &= [k_A + h(d_A \parallel ID_A)]G \\ &+ [(q_{ax} + h(ID_A))]PK_{AC} \end{aligned} \quad (18)$$

$$\because V_A = h(d_A \parallel ID_A)G \quad (19)$$

$$\because PK_A = V_A + (k_A - h(ID_A))G \quad (20)$$

$$V_A = PK_A - (k_A - h(ID_A))G \quad (21)$$

$$\begin{aligned} S_A &= k_A G + V_A \\ &+ [(q_{ax} + h(ID_A))]PK_{AC} \end{aligned} \quad (22)$$

$$\begin{aligned} S_A &= PK_A + h(ID_A)G \\ &+ [(q_{ax} + h(ID_A))]PK_{AC} \end{aligned} \quad (23)$$

U_A 與驗證中心(AC)註冊，一旦各使用者自驗證中心完成註冊並取得屬於自己的公鑰 PK_n 及簽章 W_n 後，則不需驗證中心於系統中執行身分驗證工作，可憑驗證中心核發的帳戶相關資料(ID_n 、 PK_n)與自行計算的公開金鑰 S_n ，逕自進行相互身分認證。

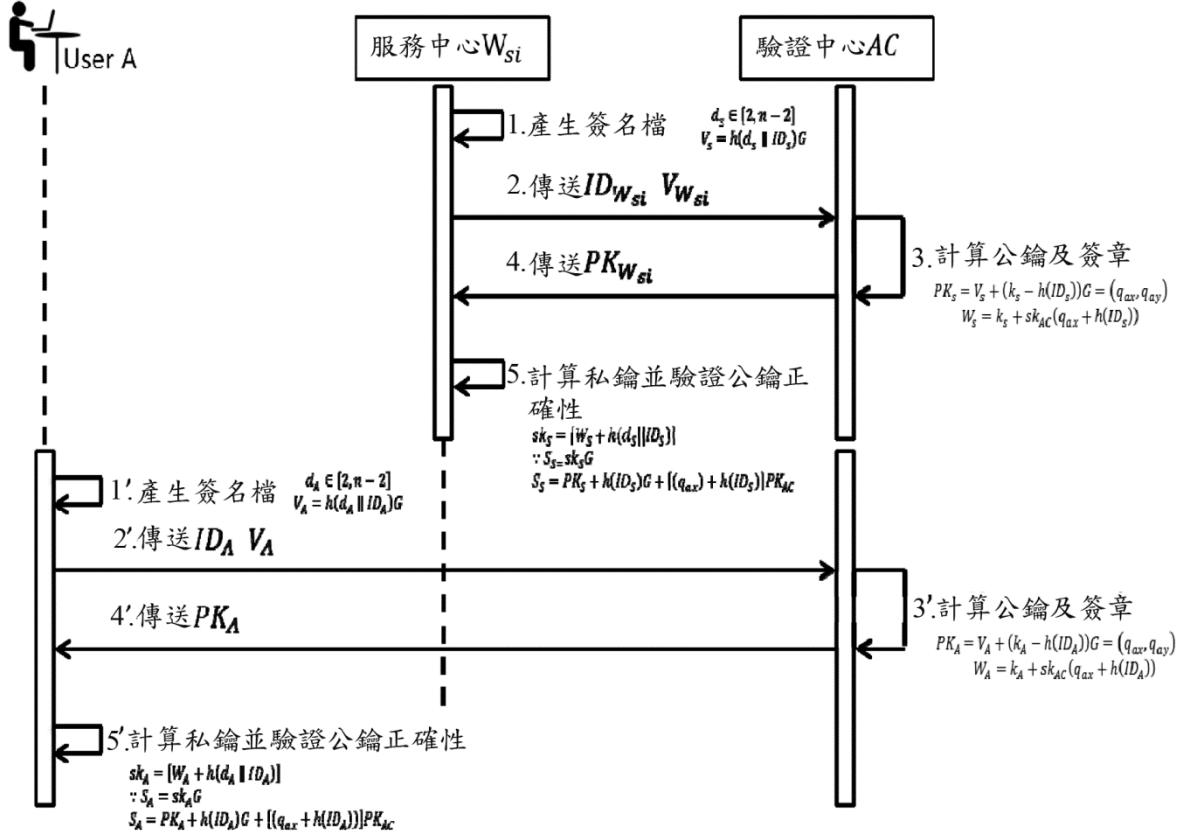


圖 5 登入註冊階段

四、存取驗證階段

U_A 與 W_{si} 自驗證中心取得合法認證身分後，使用者可憑帳戶資料與服務中心 W_{si} 進行相互身分驗證，在產生共享秘鑰 $K_{(A,S)}$ 前，服務中心需與 U_A 相互確認 (ID_A, S_A, PK_A) 及 (ID_S, S_S, PK_S) 是否正確，驗證無誤後即可建立共享秘鑰 $K_{(A,S)}$ ，如圖 6。驗證檢查式如下：

$$S' = PK_A + h(ID_A)G + [(q_{ax} + h(ID_A))]PK_{AC} \quad (24)$$

$$S'_A \stackrel{?}{=} S_A \quad (25)$$

同樣的， U_A 也可驗證 $S'_S \stackrel{?}{=} S_S$ ，經過彼此驗證為合法使用者及服務中心後，即可建立共享秘鑰 $K_{(A,S)}$ 。

$$K_{(A,S)} = sk_A \times S_S = sk_S \times S_A \quad (26)$$

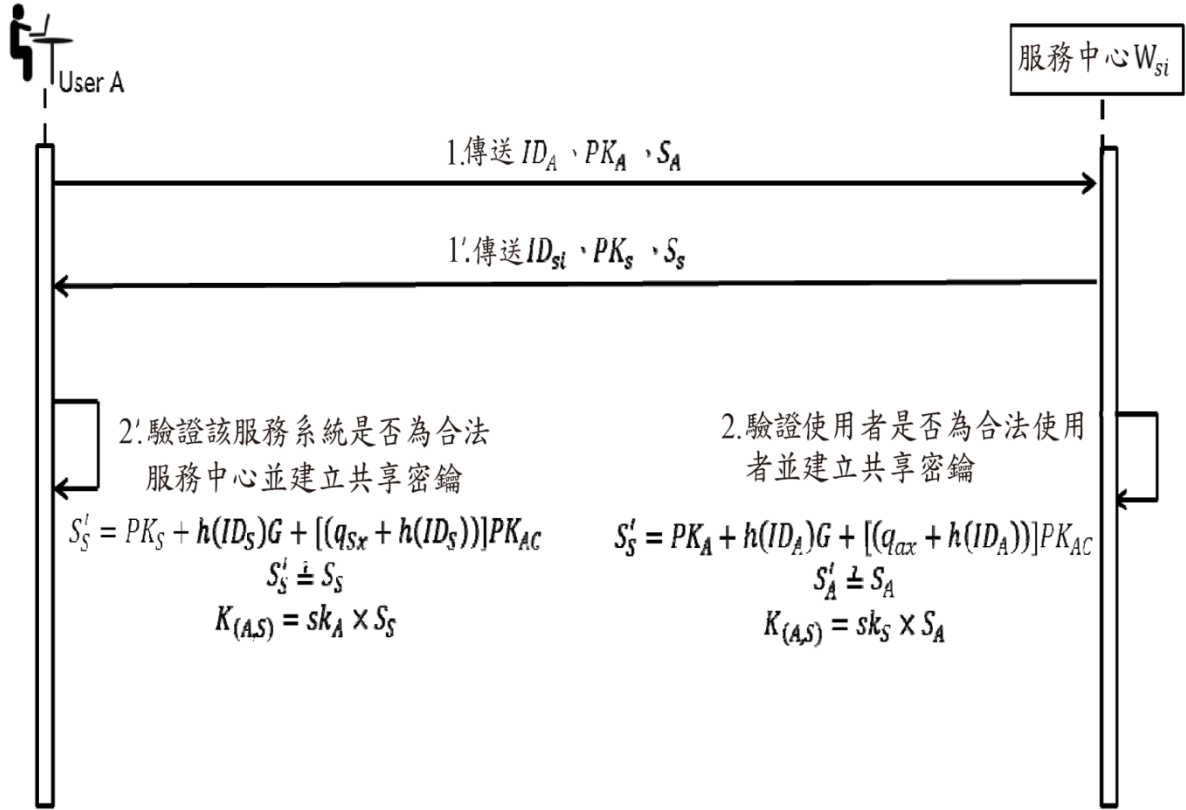


圖 6 服務中心存取驗證階段

五、存取驗證階段

使用者提出服務使用申請，取得服務使用及權限種類序列，並依照需求將授權服務及存取權限值加密後傳送服務中心要求服務使用，服務中心解密後依照授權服務及存取權限值提供服務，如圖 7。

步驟一： U_A 向服務中心申請服務，服務中心 W_{Si} 將授權服務序列 A 及服務存取權限種類序列 B 傳送給 U_A 。

步驟二： U_A 收到授權服務序列 A 及服務存取權限種類序列 B 時，計算服務之使用權限值及存取權限種類值。

➤ 依使用需求建立服務使用權限 t_{U_A} ，並與授權服務序列 A 計算使用權限值。

$$A = (a_1, a_2, \dots, a_n), \quad 0 \leq a_i \leq g_n f_n - 1 \quad (27)$$

$$t_{U_A} = (t_1, t_2, \dots, t_n), t_n \in [0,1] \quad (28)$$

$$A'f = \sum_{i=1}^n A \times t_{U_A} \quad (29)$$

➤ 依使用需求建立存取權限種類 $t_{U_A}^*$ ，並與權限種類序列 B 計算權限種類值。

$$B = (b_1, b_2, \dots, b_m), \quad 0 \leq b_i \leq g_m f_m - 1 \quad (30)$$

$$t_{U_A}^* = (t_1, t_2, \dots, t_m), t_m \in [0,1] \quad (31)$$

$$A't = \sum_{i=1}^m B \times t_{U_A}^* \quad (32)$$

步驟三： U_A 隨機擇一參數 k'_A ，令權限明文成為點訊息，並計算使用者權限密文。

$$M = ((A'f, A't) + K_{(A,S)}) = (m_1, m_2) \quad (33)$$

$$C_{A_1} = k'_A \times G \quad (34)$$

$$Y_A = (y_{A_1}, y_{A_2}) = k'_A \times S_S \quad (35)$$

$$C_{A_2} = (C_{21}, C_{22}) = (y_{A_1} \times m_1 \bmod q, y_{A_2} \times m_2 \bmod q) \quad (36)$$

$$C_{A_0} = (C_{A_1}, C_{A_2}) \quad (37)$$

步驟四：使用者傳送權限密文 C_{A_0} 給服務中心。

步驟五：服務中心接收到使用者傳送的權限密文 C_{A_0} 後，解開 C_{A_0} 內容。

➤ 服務中心以私鑰 sk_S 計算 Z 值。

$$Z = sk_S \times C_{A_1} = (Z_1, Z_2) \quad (38)$$

➤ 服務中心利用共享秘鑰 $K_{(A,S)}$ ，以(39)(40)式計算，即可得到服務使用權限及權限種類值。

$$M = (C_{21} \times Z_1^{-1} \bmod q, C_{22} \times Z_2^{-1} \bmod q) = (m_1, m_2) \quad (39)$$

$$(A'f, A't) = (m_1, m_2) - K_{(A,S)} \quad (40)$$

➤ 依服務使用權限及權限種類值，以(41) - (46)式計算，即可得到服務使用權限及權限種類。

$$c_{g_n} = A'f \bmod g_n, 0 \leq c_{g_n} < g_n - 1$$

$$c_{f_n} = A'f \bmod f_n, \frac{c_{f_n}}{2} < c_{f_n} \leq \frac{c_{f_n}}{2} \quad (41)$$

$$(c_{g_n} - c_{f_n})_2 = t_{U_A} = (t_1, t_2 \dots, t_n), t_n \in [0, 1] \quad (42)$$

$$c_{g_m} = A't \bmod g_m, 0 \leq c_{g_m} < g_m - 1 \quad (44)$$

$$c_{f_m} = A't \bmod f_m, \frac{c_{f_m}}{2} < c_{f_m} \leq \frac{c_{f_m}}{2} \quad (45)$$

$$(c_{g_n} - c_{f_n})_2 = t_{U_A}^* = (t_1, t_2 \dots, t_m), t_m \in [0, 1] \quad (46)$$

步驟六：服務中心依服務使用權限值 t_{U_A} ，判定使用者對哪些服務具使用權限，並依權限種類值 $t_{U_A}^*$ 判定使用者對授權服務具有哪些存取權限種類。

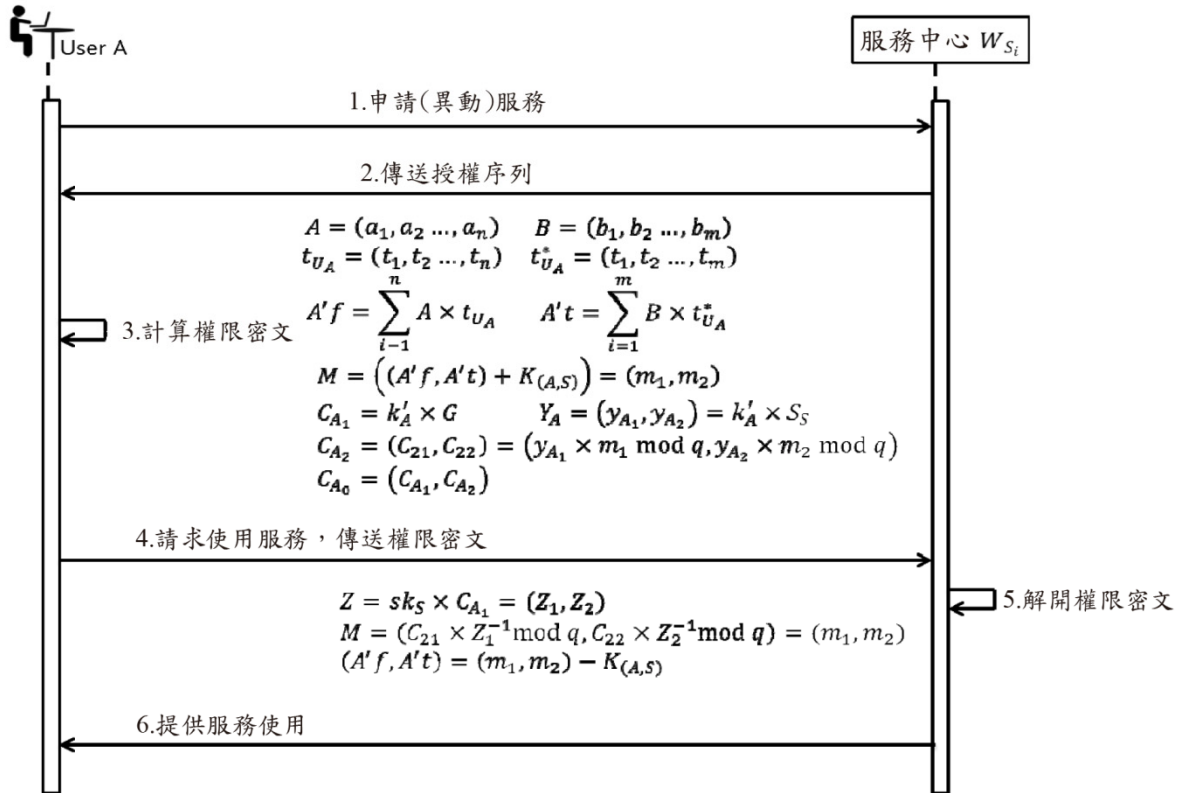


圖 7 服務存取階段

六、導入飛航管制模擬訓練系統

配合雲端環境將上述存取控制方法導入於空軍飛航管制模擬訓練系統，如圖 8，飛航管制模擬訓練服務中心存取循序圖。運用本研究之動態存取控制相對於傳

統的存取控制，能提供較彈性的服務及便利性，並且給予權限合理的分配，能讓合法使用者安全使用，提高整個系統的安全性。

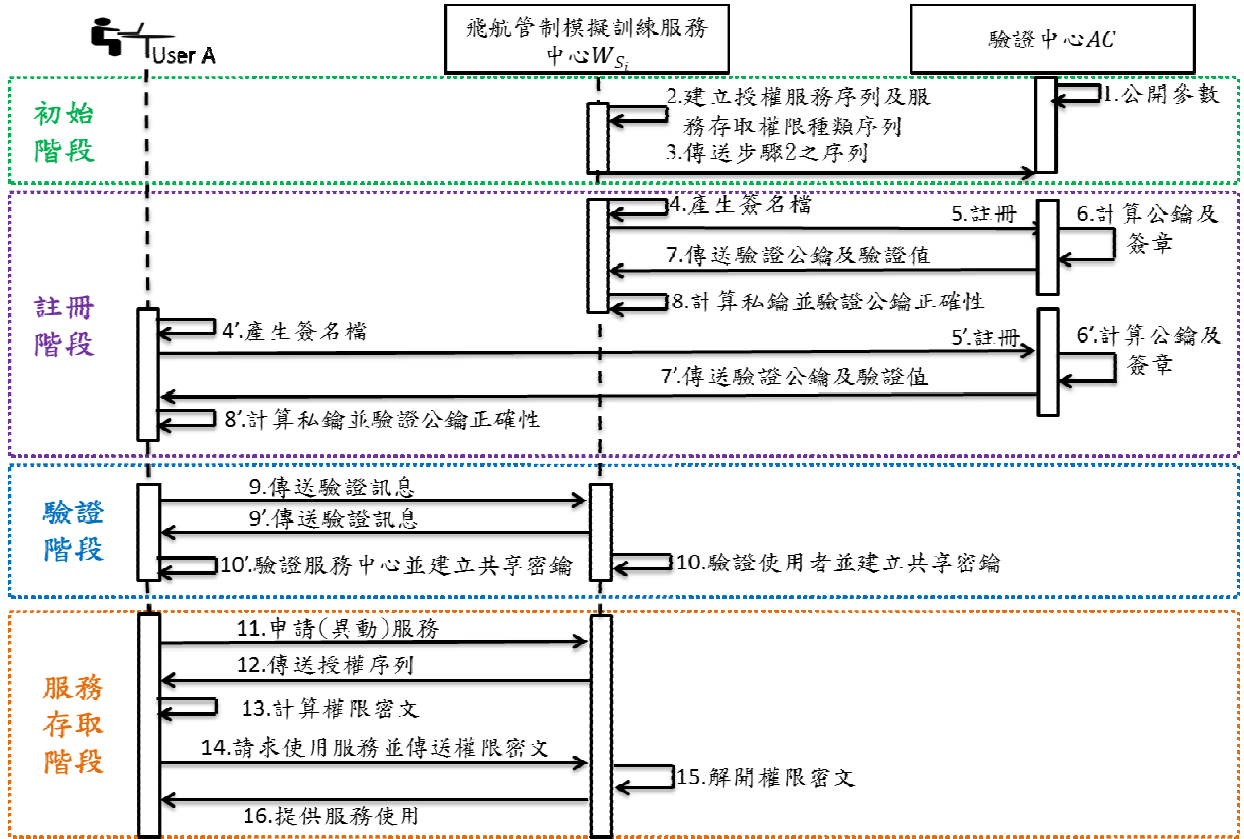


圖 8 飛航管制模擬訓練服務中心存取循序圖

(一)飛航管制模擬訓練服務中心存取流程

(1)至(9)：飛航管制模擬訓練服務中心完成序列建置並傳予驗證中心供使用者查詢。

(10)至(23)：使用者與飛航管制模擬訓練服務中心分別向驗證中心完成註冊。

(24)至(26)：使用者與飛航管制模擬訓練服務中心各自驗證雙分身是否正確合法。

(27)至(46)：使用者申請(異動)服務，並由飛航管制模擬訓練服務中心完成服務提供。

(二)系統初始階段

系統初始階段包含系統建置階段、飛航管制模擬訓練服務中心(W_{Si})建置服務及權限序列，系統初始階段如上。

(三)登入註冊階段

在登入階段，使用者 U_A 及服務中心

W_{Si} 向驗證中心註冊，參與金鑰建置，使用者註冊詳細階段請參考三、登入註冊階段。服務中心註冊如圖9。步驟分述如下：

步驟一：服務中心 W_{Si} 以自己 $ID_{W_{Si}}$ 及隨機參數 $d_{W_{Si}}$ ， $d_{W_{Si}} \in [2, n-2]$ ，透過單向無碰撞雜湊函數 $h()$ 產生簽名檔 $V_{W_{Si}}$ ，並將 $ID_{W_{Si}}$ 與 $V_{W_{Si}}$ 傳給驗證中心。

$$V_{W_{Si}} = h(d_{W_{Si}} || ID_{W_{Si}})G \quad (47)$$

步驟二：驗證中心(AC)選擇一隨機數值 $k_{W_{Si}} \in [2, n-2]$ 計算 W_{Si} 之驗證公鑰 $PK_{W_{Si}}$ 及簽章 $W_{W_{Si}}$ 後傳給 W_{Si} ，計算式如下：

$$\begin{aligned}
PK_{W_{S_i}} &= V_{W_{S_i}} \\
&+ \left(k_{W_{S_i}} \right. \\
&\quad \left. - h \left(ID_{W_{S_i}} \right) \right) G \\
&= (q_{ax}, q_{ay})
\end{aligned} \tag{48}$$

$$\begin{aligned}
W_{W_{S_i}} &= k_{W_{S_i}} \\
&+ sk_{AC} \left(q_{ax} \right. \\
&\quad \left. + h \left(ID_{W_{S_i}} \right) \right)
\end{aligned} \tag{49}$$

步驟三： W_{S_i} 利用 AC 傳回之參數 $(ID_{W_{S_i}}, V_{W_{S_i}})$ 自己計算私鑰 $sk_{W_{S_i}}$ ，並利用簽章 $W_{W_{S_i}}$ 驗證公鑰 $PK_{W_{S_i}}$ 的正確性，計算式如下： $sk_{W_{S_i}} =$

$$\left[W_{W_{S_i}} + h \left(d_{W_{S_i}} || ID_{W_{S_i}} \right) \right] \tag{50}$$

證明式如下：

$$\because S_{W_{S_i}} = sk_{W_{S_i}} G \tag{51}$$

$$\begin{aligned}
S_{W_{S_i}} &= \left[k_{W_{S_i}} + sk_{AC} \left(q_{ax} + h \left(ID_{W_{S_i}} \right) \right) \right. \\
&\quad \left. + h \left(d_{W_{S_i}} || ID_{W_{S_i}} \right) \right] G
\end{aligned} \tag{52}$$

$$\begin{aligned}
S_{W_{S_i}} &= \left[k_{W_{S_i}} \right. \\
&\quad \left. + sk_{AC} \left(q_{ax} + h \left(ID_{W_{S_i}} \right) \right) \right] G \\
&\quad + h \left(d_{W_{S_i}} || ID_{W_{S_i}} \right) G
\end{aligned} \tag{53}$$

$$\begin{aligned}
PK_{AC} = sk_{AC} G(54) S_{W_{S_i}} &= \\
\left[k_{W_{S_i}} + h \left(d_{W_{S_i}} || ID_{W_{S_i}} \right) \right] G \\
+ \left[\left(q_{ax} + h \left(ID_{W_{S_i}} \right) \right) \right] PK_{AC}
\end{aligned} \tag{54}$$

$$\because V_{W_{S_i}} = h \left(d_{W_{S_i}} || ID_{W_{S_i}} \right) G \tag{55}$$

$$\begin{aligned}
&\because PK_{W_{S_i}} \\
&= \\
V_{W_{S_i}} + \left(k_{W_{S_i}} - h \left(ID_{W_{S_i}} \right) \right) G
\end{aligned} \tag{56}$$

$$\begin{aligned}
V_{W_{S_i}} &= \\
PK_{W_{S_i}} - \left(k_{W_{S_i}} - h \left(ID_{W_{S_i}} \right) \right) G
\end{aligned} \tag{57}$$

$$\begin{aligned}
S_{W_{S_i}} &= k_{W_{S_i}} G + V_{W_{S_i}} \\
&+ \left[\left(q_{ax} \right) + h \left(ID_{W_{S_i}} \right) \right] PK_{AC}
\end{aligned} \tag{58}$$

$$\begin{aligned}
S_{W_{S_i}} &= PK_{W_{S_i}} + h \left(ID_{W_{S_i}} \right) G \\
&+ \left[\left(q_{ax} \right) + h \left(ID_{W_{S_i}} \right) \right] PK_{AC}
\end{aligned} \tag{59}$$

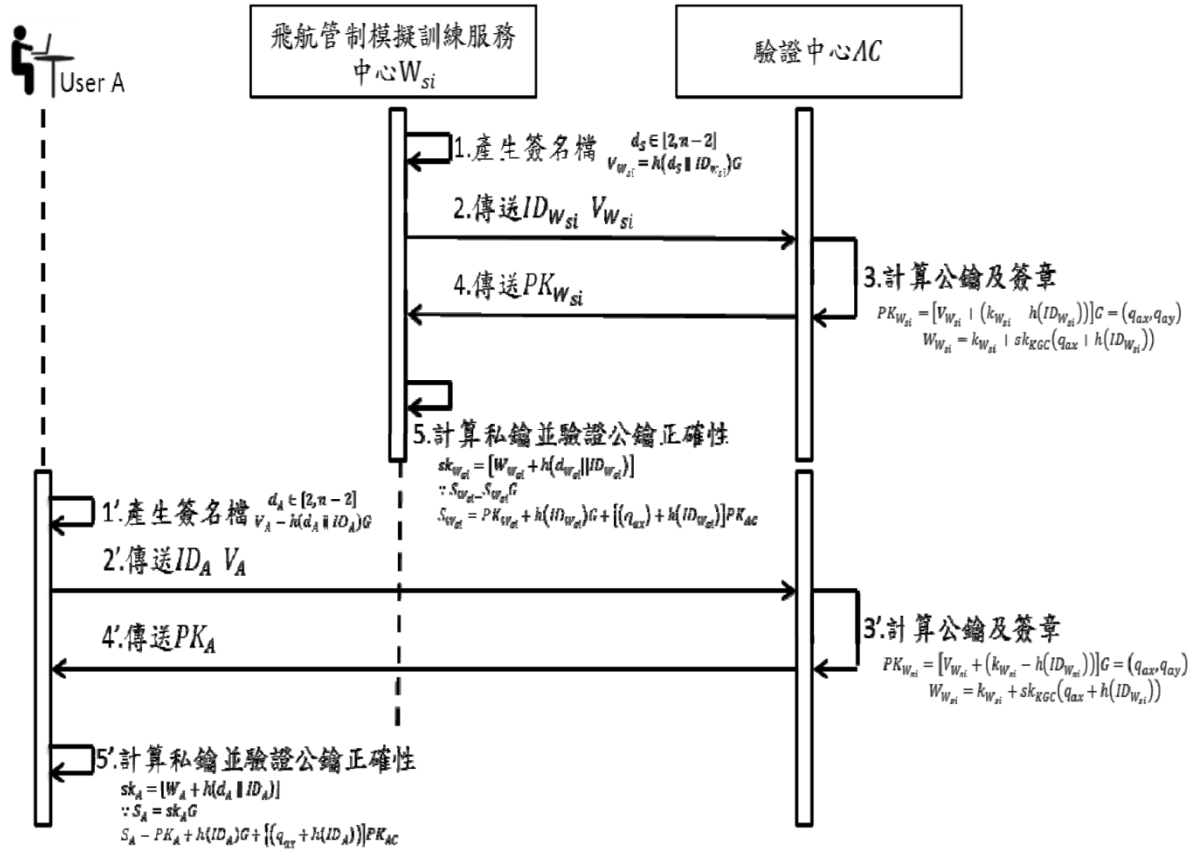


圖 9 飛航管制模擬訓練服務中心註冊階段

七、飛航管制模擬訓練服務存取階段

當使用者申請使用服務時，經取得服務使用及權限種類序列後，依照需求將授權服務及存取權限值加密後傳送飛航管制模擬訓練服務中心要求服務使用，該服務中心解密後依照授權服務及存取權限值提供服務。服務存取階段如圖 9。

肆、安全性及效益分析

針對本研究之存取控制在雲端環境下，運用於飛航管制模擬訓練系統時，針對系統的「安全性分析」及「效益分析」等相關內容進行探討與比較，分別說明如下：

一、安全性分析：

本研究之重點著重於飛航管制模擬訓練系統在雲端環境下，就人員存取控制權限以獲得授權服務方面而言，其結果根據國際標準組織(International Standards Organization, ISO)組織所提出資訊系統安全管理需求，一個安全的資訊系統應該

要達到的機密性、完整性、不可否認性等三方面外，另增加身分認證、存取控制、雙重破密難題及避免同謀攻擊等進行安全探討，分別說明如下：

(一)機密性(Confidentiality)

機密性指的是資料不得被未經授權之個人、實體或程序所取得或揭露的特性，資料在成功傳遞至目的地之後，所有的資料交換都是保密的。本方法中有關權限密文傳輸，由於使用了橢圓曲線公開金鑰之加密方法，使用者須將所需使用之服務及權限種類序列值($A'f, A't$)與共享密鑰 $K_{(A,S)}$ 執行橢圓曲線點加法運算，運算編碼如(33)式：

$$M = ((A'f, A't) + K_{(A,S)}) = (m_1, m_2)$$

假如破譯者想解開這些資訊，將面臨橢圓曲線離散對數難題(ECDLP)，首先需經由破解(34)、(35)與(36)式後，再從(33)式中設法得知使用者之服務使用及權限種類值($A'f, A't$)與取得雙方共享金鑰

$K_{(A,S)}$ ；即使破譯者不管運用何種方法取得使用者服務使用及權限種類值 $(A'f, A't)$ ，仍然將會再面臨到隨機背包難題，而如何從服務使用及權限種類值 $(A'f, A't)$ 導出服務使用及權限種類序列是很困難的，因為這類的問題已經被證實是一個 NP-Complete 問題，無法在多項式時間內解決。

(二)完整性(Integrity)

完整性係指訊息在傳遞過程中不能被破壞或干擾，通訊的內容在通訊節點間傳遞的過程中確認沒有被改變，也就是訊息在的處理過程中不能被加入、刪除或修改。因此，針對本研究中，假若破譯者想偽冒使用者身分發送訊息給管理者，除非獲得使用者個人申請認證之資訊，否則傳送至驗證中心之存取權限是無法被更改的。

就本方法的註冊過程，使用者經由(10)式： $V_A = h(d_A \parallel ID_A)G$ 將自己的簽名檔傳送給對方(驗證中心)，對方(驗證中心)也將使用者身分訊息進行雜湊運算，再結合使用者簽名檔 V_A 經由(11)式： $PK_A = V_A + (k_A - h(ID_A))G = (q_{ax}, q_{ay})$ 運算後並回傳，若第三方想要從中介入偽冒或竄改使用者簽章而不被發現情況下，則他將面對破解單向雜湊函數(OWHF)及橢圓曲線離散對數難題(ECDLP)；即便是破譯者成功偽冒使用者身分發送服務使用及權限給服務中心或是竄改權限，除非獲得使用者個人申請認證之私鑰，或是破解 C_{A_0} 內容後所取得的共享秘鑰 $K_{(A,S)}$ ，否則他將面臨著破解橢圓曲線離散對數難題(ECDLP)，而在未破解的前提下傳送至服務中心之服務使用及權限是無法被更改或偽冒的。

(三)可用性(Availability)

確保資訊與系統持續運轉無誤，當合法使用者要求使用資訊系統時，使用者均可在適當的時間內獲得回應，並完成服務需求。

本研究在使用者與服務中心兩者雙方完成身分驗證確認為合法後，如(23)式：

$$S_A = PK_A + h(ID_A)G + [(q_{ax} + h(ID_A))]PK_{AC}, \text{ 服務中心即可依使用者提出之服務申請權限密文，並將其解開後，依內容提供服務，如(40)式 } (A'f, A't) = (m_1, m_2) - K_{(A,S)}$$

(四)不可否認性(Non-repudiation)

不可否認性指的是對一已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。在驗證中心所獲得之權限密文中，包含使用者與管理者雙方共享秘鑰。在共享秘鑰內含雙方傳給認證中心之公鑰。

在服務請求過程中，權限密文 C_{A_0} 包含使用者與服務中心雙方產生之共享秘鑰 $K_{(A,S)}$ ，如(33)式：

$$M = ((A'f, A't) + K_{(A,S)}) = (m_1, m_2)$$

而在共享秘鑰的組成內含雙方秘密保管之私鑰及公開之公鑰如(26)式：

$$K_{(A,S)} = sk_A \times S_S = sk_S \times S_A$$

，其中由於私鑰是由使用者利用身分資料來參與金鑰建置，因此已經將個人資訊隱含在內如(13)式： $sk_A = [W_A + h(d_A \parallel ID_A)]$ ，使用者無法否定曾經提出的服務請求或掩飾使用過該服務。

(五)身分認證(Authenticity)

身分認證指的是可以提供線上另一使用者的確認性服務，在連線過程中提供發送者或接收者的身分確認。本研究設計了公正的第三方驗證中心，因此想要獲取服務使用之使用者或是提供服務之服務中心都必須透過它註冊。

藉由本身的身分資料或隱藏之身分資料建立驗證公鑰如(11)式：

$$PK_A = V_A + (k_A - h(ID_A))G = (q_{ax}, q_{ay})$$

，而之後即便雙方都需要再進行資料傳輸時，就可利用彼此的身分資料及驗證公鑰，同時逕自驗證雙方是否均為合法使用者如(23)式：

$$S_A =$$

$$PK_A + h(ID_A)G + [(q_{ax} + h(ID_A))]PK_{AC}$$

而不再需再透過公正之第三方做保證與協調作業。所以本方法之身分認證，只要持有驗證中心之公鑰 PK_{AC} 即可透過雙方

傳遞之身分資料、公鑰及驗證公鑰快速執行身分確認。

(六)存取控制(Access Control)

存取控制指的是存取權限值管理上的安全，它除了必須符合設定合法使用者所具有的存取權限外，還必須判斷服務請求是否符合所授權的權限。本研究所提出的存取控制方法，係利用序列方式代表授權物件與權限範圍，使用者可依照需求建立另一序列，同時該序列僅以 1 或 0 來表示是否具備該物件之使用及相關權限，再結合隨機背包密碼系統以求得服務使用及權限種類值，做為服務請求判斷及存取權限範圍，如(29)式： $A'f = \sum_{i=1}^n A \times t_{U_A}$

及(32)式 $A't = \sum_{i=1}^m B \times t_{U_A}^*$ ，這種方式可以讓服務供應方在使用者所註冊的合理授權範圍之下，提供使用者服務使用及權限選擇之彈性。

本研究將利用序列代表授權物件與權限範圍，使用者可依需求建立另一序列，該序列僅以 1 或 0 表示是否具該物件之使用及相關權限，不同於傳統及後續衍生之存取控制方法需明確使用者具那些物件或權限，其優點讓使用者在使用該物件或權限異動時更具彈性。經比較傳統存取控制方法優缺點，如表 3。

表 3 存取控制方法優缺點比較表

優缺點 方法	優點	缺點
存取控制 矩陣	簡單易用	在一個龐大的系統中，當主體使用的資源不夠多時，所建立的存取控制矩陣將會形成資料結構中的稀疏矩陣(Sparse Matrix)，非常浪費龐大的記憶體空間，或當使用者或系統資源一旦過多時，矩陣會變得過於龐大而不易管理。
存取控制 串列	以物件角度來管理與維護權限容易且簡單。	若以主體角度檢視某主體所擁有的物件與權限，須先檢索全部物件串列後才可得知主體對物件之權限是其缺點，因此若變更主體權限較頻繁時，會造成管理上負擔。
能力串列	以使用者角度可輕易且簡單的管理與維護權限。	若頻繁的變更物件權限，將造成時間的耗費與管理者的負擔與困擾。
鎖碼 核對法	不同傳統方式去作表格或串列的查詢，另外鍵值與鎖值均由亂數所組成，較具安全性。	無法任意增加或刪除使用者或檔案，因為加入或刪除動作會牽動許多已經存在的鍵值及鎖值，幾乎要重新計算鍵值及鎖值。

(七)雙重破密難題(Dual Decrypted Complications)

雙重破密難題指運用雙重密碼設計防止第三者截獲後輕易破解機制。本方法在開始產生服務序列階段時，係利用隨機背包密碼系統，先完成服務使用及權限種類範圍序列建置，使用者再依需求建立服務使用及權限種類值，並透過橢圓曲線密碼系統(ECC)將服務使用及權限種類值加

密後，重送權限密文給服務中心請求服務。

如(33)式：

$$M = \left((A'f, A't) + K_{(A,S)} \right) = (m_1, m_2)$$

演算所表示之權限密文可知，即便破譯者攔截權限密文並破解橢圓曲線離散對數難題(ECDLP)後，仍得要面臨破解隨機背包難題(RKP)。

(八)避免同謀攻擊 (Avoid Collusion Attacks)

同謀攻擊係指第三者試圖在密碼雜湊中找出相同的輸入雜湊值。本方法中使用者在註冊階段時，會將自己的身分資料經雜湊後，將簽名檔如(10)式：

$V_A = h(d_A \parallel ID_A)G$ 傳送給驗證中心參與金鑰建置，而並非由驗證中心產生並管理公鑰或私鑰，如此可避免內部相關管理人員監守自盜情況發生。

另外在服務提供過程中，權限密文是透過共享密鑰方式加密如(26)式： $K_{(A,S)} = sk_A \times S_S = sk_S \times S_A$ ，驗證中心僅止於參與公鑰與私鑰建置，因此無法得知共享密鑰進而奪權；此外，由於服務中心僅提供授權服務使用及權限種類之範圍，並無明確管理使用哪些服務及權限，可有效避免後端管理者藉由管理之便，進而盜用使用者權限。

表 4 本研究與現行方法安全性比較表

就人員存取控制權限以獲得授權服務面向比較		
比較項目	現行飛航管制模擬訓練系統	本研究方法
機密性	易曝露使用者身分及訓練等級。	使用橢圓曲線密碼系統加密，可減少於有限之頻寬內之資訊耗費。
完整性	無法確保人員資料在傳遞過程中是否被竄改。	必須面對破解單向雜湊函數的問題及面對橢圓曲線離散對數問題，所以可以確保完整性。
可用性	使用者透過申請註冊後，於服務系統開放該使用者身分使用服務。	使用者與服務中心兩者雙方完成身分驗證確認為合法後，服務中心依服務申請權限密文，提供服務。
不可否認性	飛航管制人員易因冒用帳號造假訓練。	在服務提供過程中，已經將個人資訊隱含在內，使用者無法否定或偽造使用過該服務。
身分認證	雙方進行資料傳輸時需再透過公正之第三方做保證與協調作業。	藉由本身的身分資料建立驗證公鑰，不再需再透過公正之第三方做保證與協調作業。
存取控制	需仰賴後端龐大資料庫權限矩陣做服務及授權範圍鑑別。	利用序列方式代表授權物件與權限範圍提供使用者服務使用及權限選擇之彈性。
雙重破密	無。	採橢圓曲線密碼及隨機背包密碼設計防止第三者截獲後輕易破解。
同謀攻擊	無。	使用者將自己的簽名檔雜湊後傳送給驗證中心參與金鑰建置，驗證中心僅止於參與公鑰與私鑰建置，因此無法得知共享密鑰。

二、效益分析：

存取控制矩陣法、存取控制串列、能力串列、授權關係表及鎖碼核對法等是類之傳統存取控制方法，仍然保有由管理端負責變更及管理使用者權限的概念，而存在著浪費記憶空間、權限異動及管理不便等問題。因此本研究提出運用動態存取控

制方法，可由使用者可以按需求在授權範圍內的服務及權限彈性調整。現特針對現行飛航管制模擬訓練系統之傳統存取控制與本研究設計之動態存取控制機制比較兩者之各項效益如下，本方法與現行方法分析比較，如表 5。

表 5 本研究與現行方法效益比較表

就人員存取控制權限以獲得授權服務之效益比較		
比較項目	現行飛航管制模擬訓練系統	本研究方法
記憶空間	存放使用者存取權限表，浪費記憶空間。	使用者可自行依其任職職務席位申請使用服務，並無存放使用者存取權限表問題，將有效節省記憶空間。
權限異動	權限異動需透由單位逐級申請，欠缺彈性。	本方法提供使用者依其需求建立權限以取得服務，有效增加權限異動彈性。
使用便利性	註冊採人工作業，作業冗長，易發生人為疏失。	自動化，作業時程短，省時省事，並可提高提高資源使用率。
訓練時間	須將人員於特定時間內，統一集中實施訓練影響單位任務人力。	人員隨時利用系統服務實施訓練。
訓練成本	需要管理人力及繁雜的文書作業往返，花費成本高。	線上作業以電子檔為主，簡化行政流程，無需龐大人力及文書紙張，花費成本低。

(一)記憶空間

記憶空間指的是後端資料庫在存放存取權限所需使用到的空間容量。在本方法中，使用者可自行依其任職職務席位申請使用服務，並無存放使用者存取權限表問題，將有效節省記憶空間。

(二)權限異動

權限異動指的是使用者在有需求的情況下，變更權限的行為。本方法提供使用者授權之服務序列及權限序列，使用者依其需求建立權限以取得服務，除在非授權服務範圍內需重新認證取得新的服務序列並重新計算權限外，完全依照使用者需求提供服務，有別於傳統存取控制方法，均須重新註冊，有效增加權限異動彈性。

(三)使用便利性

使用性指的是存取控制方法在使用上的便利性。本方法在使用上僅透過服務序列及權限序列來計算權限值，使服務的提供將更具便利性。

(四)訓練時間

原訓練方式須將人員定期召集後，統一集中實施訓練，時間固定不具彈性，且相對影響單位任務人力運用。本方法可由

人員自行安排時間，隨時利用系統服務實施訓練。

(五)訓練成本

原系統相關註冊及服務申請均需要後端管理人力及繁雜的文書作業往返，花費成本高。本研究所使用之服務採線上作業並以電子檔為主，簡化行政流程，無需龐大人力管理及文書紙張，花費成本低。

三、計算成本分析：

系統資源的存取管控機制已經是一個重要的議題。在本論文中提出一套加密機制的存取控制概念，作為系統安全管控的方式，如此不僅能確保系統資源的安全性，更能讓管理者有效地管理系統。而探討多數存取控制方法仍然植基於傳統的存取控制矩陣法、存取控制串列及能力串列，屬於空間複雜度的探討，而飛航管制模擬訓練系統由於尚未建置完成，惟基於未來該系統發展方便檢視對照，因此我們立基於時間複雜度觀點的考量，與現行飛航管制模擬訓練系統進行分析比較，以供後續研究參考，表 6 為時間複雜度運算參考表、表 7 為服務中心內部存取時間複雜度比較表。

表 6 時間複雜度運算之相互關係參考表

符號	定義	運算時間
T_{MUL}	進行一次模式乘法運算所需時間	$= T_{MUL}$
T_{EXP}	進行一次模式指數運算所需時間	$\approx 240 T_{MUL}$
T_{ADD}	進行一次模式加法運算所需時間	(可忽略不計)
T_{INVS}	進行一次模式乘法反元素所需時間	$\approx 240 T_{MUL}$
T_{ECMUL}	進行一次 ECC 乘法運算所需時間	$\approx 29 T_{MUL}$
T_{ECADD}	進行一次 ECC 加法運算所需時間	$\approx 5 T_{MUL}$
T_h	進行一次點 hash 所需時間	$\approx 23 T_{MUL}$
t_h	進行一次 hash 所需時間	$\approx 0.4 T_{MUL}$
附註: 因模數加法、模數減法運算時間低, 予以忽略不計		

表 7 存取時間複雜度比較表

演算法	飛航管制模擬訓練系統		本研究	
比較項目	時間複雜度	概估	時間複雜度	概估
金鑰產生	未提供演算法		$3T_{ECADD} + 2t_h$	$\approx 2.36 T_{MUL}$
加密運算			$1T_{ECADD}$	可忽略不計
解密運算			$2T_{ECMUL}$	$\approx 58 T_{MUL}$
驗證運算			$3T_{ECADD} + 2t_h$	$\approx 2.36 T_{MUL}$
合計			$\approx 62.72 T_{MUL}$	

伍、結論及未來研究方向

因我國與中共兩岸關係平緩，國軍因應精粹案等政策實施逐漸邁向小而精、而強的體制規劃，如何運用有限的資維持甚至開創強大的訓練能量是當務之急，而本研究目標則是針對此狀況下，量身訂作，針對飛航管制模擬訓練系統，建置一適雲端環境，搭配存取控制機制及橢圓曲線密碼系統具有之短長度金鑰與低計算複雜度特性配合背包序列之動態性質，來設計本系統，在最節省資源狀況下，符合現今空軍需求，綜整本研究貢獻如下：

一、針對跨組織架構的個人資料存取，透

過加密機制，並在存取控制有效率的雲端運算環境下，讓使用者能放心安然而就傳統存取控制方法的觀點來看，存取權限的管理仍需要仰賴後端龐大的資料庫，易衍生浪費龐大的記憶體空間及權限異動造成等問題。因此一套完善的雲端運算環境，必須考量後端存取控制的安全性與適切性，存取權限及金鑰管理等皆需大量仰賴後端的安全管理機制及資料庫的全使用相關資源。

二、管理端權限大幅下修，僅剩餘授權服務的範圍及權限種類，以避免內部權

- 限管理風險，減少洩違密情事發生。
- 三、為了避免金鑰集中管理，將共享密鑰運用於針對權限密文加密，大幅度降低外洩風險。
- 四、攻擊者想要得知服務及權限內容，必須面對隨機背包之難題，因本研究設計除了將授權服務及權限已運用此機制設計，並將之資訊隱藏。
- 五、更人性化設計，針對授權範圍內的服務及權限，使用者可隨時異動，增加使用彈性。

陸、國防領域之應用

本研究探討以動態存取控制，設計空軍航管模擬訓練系統之雲端環境，屬於密碼學上的應用，結合密碼學領域中「動態存取控制」、「橢圓曲線」、「隨機背包」與「Girault 自我認證公開金鑰密碼系統」等知識，旨在建立一套適切的系統，在未來國軍人力精簡的狀況下，在不影響軍中戰訓本務，同時兼顧人性化設計、權限控管及保密安全等考量，期能符合未來國軍建軍備戰的目標。

參考文獻

- 王保倉、韋永壯、胡予濮，2010，基於隨機背包的公鑰密碼，電子與信息學報，第 32 卷第 7 期：1580-1584 頁。
- 朱近之主編，2010，智慧的雲端運算－成就物聯網的未來基石，新北市：博碩文化。
- 空軍飛航管制模擬訓練系統，2011，委製協議書修訂版：26 頁。
- 郭文雄，2011，設計具自我認證之國軍網路申訴制度安全機制探討，國防大學管理學院資訊管理學系碩士論文。
- 郭儒學，2012，設計具自我認證機制且適用於網路隔離政策之雲端服務－以行政院海岸巡防署為例，國防大學管理學院資訊管理學系碩士論文。
- 陳滢等著，2010，雲端策略－雲端運算與虛擬化技術，台北市：天下雜誌。
- 陳文彬，2012，運用動態存取控制方法於雲端服務之研究，國防大學管理學院資訊管理學系碩士論文。
- 曹偉駿，黃美治，2010，適用於網路服務之高效率整合式存取控制系統設計與實作，管理與系統，第 17 卷，第 1 期：159-182 頁。
- 彭秀琴、張念慈，2010，雲端運算下資訊安全之探討，經建會管制考核處。
- 趙立威、方國偉，2011，讓雲觸手可及之微軟雲端運算實踐指南，新北市：博碩文化。
- 蔡一郎，2010，雲端運算與雲端安全架構，Communications of the CCISA，第十六卷，第四期：84-93 頁。
- 詹子銘，2013，建構專業型雲端運算平台之技術探討，新新季刊，第 41 卷第 1 期：23-38 頁。
- 樊國禎、陳祥輝、蔡敦仁，2000，資料庫濫用軌跡塑模，電腦與通訊，第 2 期：9-18 頁。
- 鄧瑋敦譯，2010，雲端運算大解密，台北市：日經 BP 社出版局編著，電腦人文化。
- 賴溪松，2003，資料庫濫用軌跡塑模，CCISA 資訊安全通訊，第 2 期：9-18 頁。
- 賴溪松、韓亮、張真誠，2004，近代密碼學及其應用，台北市：旗標出版股份有限公司。
- 廖家宏，2011，植基於橢圓曲線之多文件偽造即停簽密機制，國防大學管理學院資訊管理學系碩士論文。
- 蘇品長、盧而輝、張克章，2004，植基於混合式技術的身分識別密碼機制，中正嶺學報，第 33 卷第 1 期：1-10 頁。
- 蘇品長，2007，植基於 LSK 和 ECC 技術之公開金鑰密碼系統，長庚大學電機工程研究所博士論文。

- Ammann, P. E. and Sandhu, R. S., 1991, "Safety Analysis for the Extended Schematic Protection Model", IEEE Computer Society Symposium, pp. 87-97.
- Almorsy, M., Grundy, J. and Ibrahim, A. S., 2011, "Collaboration-Based Cloud Computing Security Management Framework", IEEE 4th International Conference on Cloud Computing, pp. 364-371.
- Diffie, W. and Hellman, M. E., 1976, "New Directions in Cryptography", IEEE Transactions on Information Theory, (IT-22:6), pp. 644-654.
- Lu, E. H., Chang, K. C., Liaw, S. H., and Su, P. C., "Proven Security and Efficiency of Gap Diffie-Hellman Group Blind Signature in E-Commerce", AMM-Applied Mechanics and Materials, (284-287), 2013, pp. 3522-3526.
- Lu, E. H., Chang, K. C., Liaw, S. H., and Su, P. C., "A Security and Efficiency of Authenticated Key Exchange Protocol for Wireless Mobile Ad Hoc Networks", AMM-Applied Mechanics and Materials, (284-287), 2013, pp. 3280-3284.
- Girault, M., 1991, "Self-Certified Public Keys", Advances in Cryptology-Eurocrypt'91, LNCS 547, pp. 490-497.
- Hwang, J. J., Shao, B. M. and Wang, P. C., 1992, "A New Access Control Method Using Prime Factorization", The Computer Journal (35:1), pp. 45-56.
- IEEE, 2000, "Standard Specifications for Public Key Cryptography", IEEE Std 1363-2000:2000.
- ISO, 1997, "Information Technology-Security Techniques-Key Management"; Part 3: Mechanisms Using Asymmetric Techniques, ISO/IEC 2nd DIS 11770-3:1997.
- ISO, 2007, "Information Technology-Security Techniques-Code of Practice for Information Security Management", ISO/IEC 27002:2007.
- Koblitz, N., 1987, "Elliptic Curve Cryptosystems", Mathematics of Computation American Mathematical Society (48:117), pp. 203-209.
- Luis, R. M., Luis, M. V., Victor G., Fermín G., Javier F., Rubén S. M., and Ignacio M. L., 2010, "From Infrastructure Delivery to Service Management in Clouds", Future Generation Computer Systems (26:8), pp. 1226-1240.
- Merkle, R. C. and Hellman, M., 1978, "Hiding Information and Signatures in Trapdoor Knapsacks", IEEE Transactions on Information Theory (IT-24:5), pp. 525-530.
- Miller, V. S., 1985, "Use of Elliptic Curve in Cryptography". Advance in Cryptology- Crypto '85, LNCS 218, pp. 417-426.
- Menezes, A. and Vanstone, S. 1993, "Elliptic Curve Cryptosystems and Their Implementation". Journal of Cryptology (6:4), pp. 209-224.
- NIST, Digital Signature Standard (DSS), FIPS PUB 186-4:2009. July 2013
- NIST, Special Publication 800-145, The NIST Definition of Cloud Computing , September 2011
- NIST, Special Publication 800-57, Recommendation for Key Management -Part 1: General (Revision 3), July 2012
- Rivest, R., Shamir, A. and Adleman, L., 1978, "A Method for Obtaining Digital Signature and Public-Key Cryptosystems", Communications of the ACM (21:2), pp. 120-126.
- Sandhu, R. S. and Samarati, P., 1994, "Access Control: Principles and Practice", IEEE Communications Magazine (32:9), pp. 40-48.

- Sutikno, S., Surya, A. and Effendi, R., 1998, "An Implementation of ElGamal Elliptic Curves Cryptosystems", 1998 IEEE Asia-Pacific Conference on Circuits and Systems, pp. 483-486.
- Subashini, S. and Kavitha, V., 2010, "A Survey on Security Issues in Service Delivery Models of Cloud Computing". Journal of Network and Computer Applications (34:1), pp. 1-11.
- Wu, T., 1993, "A Refined Key-Lock Access Control System", Aerospace and Electronics Conference (1), pp. 583-587.
- Zaborovsky, V. Lukashin, A. Kupreenko, S. and Mulukha, V., 2011, "Dynamic Access Control in Cloud Services", 2011 IEEE International Conference on Man, and Cybernetics (SMC), pp. 1400-1404.
- Administrator, "So what is the Cloud? ", Application Management and Development, 1998 (available online at <http://www.msmsoftware.com/2010/3/10/so-what-is-the-cloud.aspx>). [visited in 2012/08/06]
- GSS 資安電子報 0057 期，資料庫解決方案白皮書，參考網址：<http://www.gss.com.tw/index.php/epaper/security/892-gss0057>[visited in 2012/08/06]
- Getaltheorie en cryptography，參考網址：http://www.fisme.science.uu.nl/nwd/nwd2006/configids/getaltheorie_cryptografie.htm
- IBM Benefits of Cloud Computing [OL], <ftp://ftp.software.ibm.com/common/ssi/sa/wh/n/diw03004usen/DIW03004USEN.PDF>[visited on 2012/3/20]
- MSDN (Microsoft Developer Network)，微軟開發網路，參考網址：<http://msdn.microsoft.com/>
- NetAdmin，網管人，參考網址：http://www.netadmin.com.tw/article_content.aspx?sn=1106020007 [visited in 2012/08/03]
- 服務平台開發人員中心，邊做邊學雲端運算 (Windows Azure Platform)，參考網址：<http://msdn.microsoft.com/zh-tw/windowsazure/gg456243>[visited in 2012/07/21]
- 游舒帆，[Cloud Computing]三種雲端服務，參考網址：<http://www.dotblogs.com.tw/jimmyyu/archive/2009/12/03/12275.aspx>[visited in 2012/3/20]
- 謝錫堃、陳柏誠，雲端計算，參考網址：<http://web1.nsc.gov.tw/ct.aspx?xItem=14873&ctNode=40&mp=1> [visited in 2012/08/02]

