跨軍種服務之國防雲設計

蘇品長　葉昱宗　黃俊傑*

國防大學資訊管理學系

摘　　要

國軍現階段在雲端化過程中，各軍種仍存在獨立作業，導致無法有效整合善用資源，其原因不外乎存取權限管控及身分認證之考量。本研究透過跨服務平台設計，使用者不僅可存取原服務中心之服務，更可補足其無法提供的服務，以有效延伸資源。針對跨服務平台間存取控制方式之安全性問題，本研究提出一個植基橢圓曲線離散對數難題(Elliptic Curve Discrete Logarithm Problem, ECDLP)的存取方法，讓使用者可以在合法的權限範圍內快速又安全的存取資料，同時建置可離線作業之身分認證機制，避免服務中斷。以救災資源為例，風災來臨前，各級部隊超前部署至各災區，常面臨氣象資源不足，而災害來臨後，災區第一線狀況掌握無法即時更新等問題，更進而著墨於未來國軍走向雲端化後，如何兼顧跨平台資源存取及資料傳遞的安全性問題。

關鍵詞：存取控制，身分認證，橢圓曲線離散對數難題

A Design of Defense Cloud Computing for Cross Military Services

Pin-Chang Su,Yui-Chong Yeh,and Chun-Chieh Huang*

Department of Information Management, National Defense University

ABSTRACT

The military services of our troops currently in the process of cloud still exist independent operations, which lead to not effectively integrate and use resources. The reason is nothing more than access control and identity certification considerations.Through cross-services platform design of our study, users can access the services of the original service centers, and also can complement the services which the center did not provide to effectively extend resources. For the security problem of the method of access control for cross-services platform, we propose an access controlling method based on elliptic curve discrete logarithm problem (ECDLP), allowing users to access information quickly and safely in the legal limit of authority, while building the identity authentication mechanism of offline operations to avoid service interruption. Take disaster relief for instance, before hurricane coming, every levels of troops deployed in advance to all the affected areas often face a lack of meteorology resources. After disaster strikes, the first line of the disaster situation cannot be real-time updates to grasp. Furthermore dwell on the future of our troops toward the cloud-based, how to balance the cross-platform access to resources and information transfer security issues.

Keywords: Access Control, Identity Authentication, ECDLP

文稿收件日期 104.04.10; 文稿修正後接受日期 105.02.18;*通訊作者
Manuscript received April 10, 2015; revised February 18, 2016;* Corresponding author

一、前言

「雲端運算」(Cloud Computing)是我國四大前瞻產業之一，政府各部會相繼投入資金與人才，擘劃出雲端發展方案。就在國軍思考如何打造一支量小、質精、戰力強的部隊同時，此熱門的研究議題正可應用於未來國軍走向資訊化、雲端化的利器之一。近年來，國防事務隨著雲端之興起，國防雲概念因運而生，尤其在民間產業雲端服務發展，如雨後春筍般愈來愈多元化，改變了人們的生活方式。對國防而言，跨軍種協同作戰將進入資訊鏈結，更能完善C^4ISR，並強化指管能力。然而，在雲端環境中，軟體在雲中運行，資料也儲存在雲裡，這樣革新的運作模式產生兩方面的安全問題，一是在傳統的觀念中，資料存放在自己可控管的環境內比存放在不熟悉、不了解的地方來的更安全，也就是傳統的用戶不放心把資料放在一個不可控制的環境；二是就政策法規層面來講，目前雲端運算環境中仍缺乏有效的規範和立法[1]。

隨著資訊演進過程，國軍在使用各類資訊服務時，單一伺服器已無法滿足現況，透過跨服務中心延伸資源之機制應運而生，使用者將不再受限於傳統單一服務資源，且可有效整合使用資源。然而，如何讓使用者在特定的權限內安全的透過跨服務中心方式存取資料，是各軍種努力導向雲端所必須面對的議題。因此，確保資料在跨服務傳輸過程中達到安全且有效率，以符合雲端服務的可攜性及安全性為本研究的動機及探討重點。本研究提出一個新的跨服務中心存取控制及相互認證機制，有效降低系統中心管理負擔，同時達到資源延伸性，並運用橢圓曲線快速指數運算及背包密碼系統加解密速度快的優點，使其更能滿足於雲端之應用環境。本研究方法架構已於實踐大學研討會發表過[2]，惟未曾探討國防事務應用層面，因此，將於本文論述如何將其應用於跨軍種資源存取，以有效未來建軍備戰資源整合利用。

本文各章節部分安排如下：在第二章，彙整本研究相關文獻及技術之探討。第三章中，提出本研究方法演算法過程。第四章中，分析本方法之安全性，並與「整合式系統」作效益分析比較。最後，第五章為本文之結論。

二、文獻探討

本章分類整理、歸納分析與本研究相關的文獻，並針對雲端運算、存取控制、及加解密原理等與本研究有關的技術，加以彙整作為本研究的基礎。分述如後：

2.1 雲端運算的定義

雲端運算有兩個面向：一個是前端所提供的服務；再者，則是後端複雜的資訊技術。嚴謹的雲端運算定義為：「透過網際網路的分散式運算架構，所提供的服務模式，並具有彈性及可擴充性的能力」，並強調「平行運算」[3]。不過現在大家對雲端採取較為寬鬆的認定態度，只要滿足彈性使用及可擴充性的特性，任何網際網路上提供的運算資源和隨選服務都視為雲端運算服務的涵蓋範圍，不一定要符合分散式電腦運算架構。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。

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[1,4]。

美國國家標準與技術研究院(National Institute of Standard and Technology, NIST)將雲端運算定義為一個模型，此模型能提供一個便利並可按需求透過網路來存取與配置的共享運算資源池(如網路、伺服器、儲存裝置、應用程式與各類服務)。這些共享運算資源可以被迅速地提供並發布，同時將管理成本或服務供應商協助最小化，強調雲端運算能按照使用者的需求，進行資源的靈活調配[5]。

雲端服務簡單區分成 IaaS (Infrastructure as a Service, IaaS)、PaaS (Platform as a Service, PaaS)、SaaS (Software as a Service, SaaS)三種，

運作方式如圖 1[6]所示，說明如後。

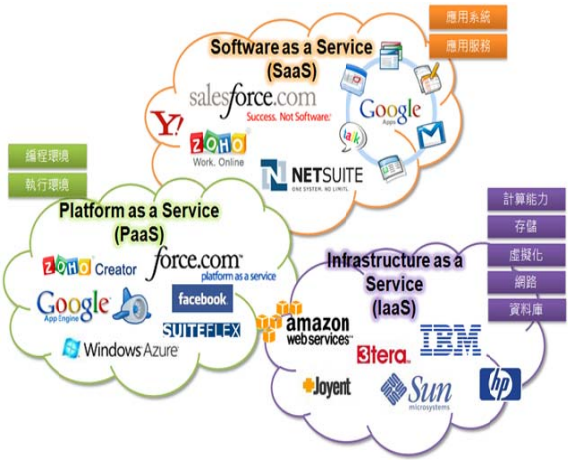


圖 1.三種雲端服務示意圖。

2.1.1 IaaS－架構即服務

IaaS 為一種服務型基礎設施(虛擬主機、網路等)。使用者透過網際網路使用雲端供應商(Cloud Provider, CP)的基礎設施。特別是虛擬化的基礎設施服務，例如 Amazon 的 EC2 等。

2.1.2PaaS－平台即服務

PaaS 為一種服務型的平台。使用者不用自己建置執行軟體的主機和作業系統(OS)等平台，透過網路使用雲端供應商(CP)的平台，可以節省主機的維管和故障排除的人力和時間，例如 Google 的 GAE(Google Application Engine)。

2.1.3SaaS－軟體即服務

SaaS 為一種服務型的軟體。使用者可下載所需軟體安裝在自己的電腦使用，或者直接透過網際網路，使用線上的軟體服務。目前服務的型態以線上使用服務居多。SaaS 的服務可以減少客戶安裝和維護軟體的時間和技能等代價，並且透過按使用計費方式來減少軟體授權費用的支出，例如微軟的 Office 等。

2.2 存取控制

資安業界有一句老話，「資安的強度，決定於最脆弱的一環。」存取控制就是資安管理中相當基礎且重要的項目，其重點涵蓋了使用者的存取管理責任、網路存取控制、系統與應用程式的存取控制等[7]。關於常見的存取控制技術有以下三項，分別說明如下：

2.2.1 存取控制矩陣(Access Control Matrix, ACM)

存取控制矩陣是最簡單的存取控制方法，也是最早被用來控制資料存取的方法；它是由一個二維陣列表現出主體(Subject)對於物件(Object)所擁有的權限，可以很清楚的把彼此間的權限表現出來，但是如果過於頻繁的更動主體與物件，將會造成系統複雜且不易維護。

2.2.2 存取控制串列(Access Control List, ACL)

存取控制串列是使用以存取控制矩陣為基礎的資料存取控制方法，每一個物件對應一個串列主體。存取控制串列描述每一個各自的存取控制列表，並記錄可以對此物件進行存取的所有主體及每個主體可以存取的權限。因此從 ACL 中可以清楚的了解每一個物件的存取控制狀況，對於整體存取控制機制管理上也很簡單。因為 ACL 是透過以物件管理而形成的串列，因此由物件的角度來管理權限是非常方便。當多個使用者對於物件有相同的存取控制權限，可讓這些使用者形成一個群組，如此一來便可簡化整個存取控制機制。

2.2.3 能力串列(Capabilities List, CL)

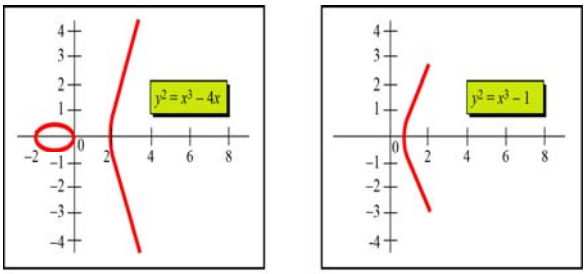
能力串列運作模式類似於 ACL，也是以存取控制矩陣為基礎的存取控制機制，但它是以主體的角度將每一個主體對應一連串的物件存取控制權限，描述每一個主體可存取的物件及權限，形成一個物件權限串列。由於主體對某個物件擁有那些存取權限不易檢閱，且對於存取權限的刪修也不方便，因此不常被使用。

2.3 密碼學相關技術

本論文相關密碼技術包含橢圓曲線公開金鑰密碼系統演算法、隨機背包密碼系統、整合式存取控制系統，以下逐一說明：

2.3.1 橢圓曲線公開金鑰密碼系統

橢圓曲線系統第一次應用於密碼學上是由Koblitz[8]與 Miller[9]分別提出，隨後有兩個較著名的橢圓曲線密碼系統被提出；一為利用ElGamal[10] 的加密法，一為Menezes-Vanstone[11]的加密法。在實數系中，橢圓曲線可定義成所有滿足方程式E:y^2=x^3+ax+b 的點(x,y)所構成的集合，如圖2 所示：



a. Three real roots　　b. One real and two imaginary roots

圖 2.橢圓曲線。

2.3.2 隨機背包密碼系統

背包難題是假設我們有一個背包它所能裝載的物品重量是固定的，但現在我們有非常多的物品，每個物品的重量都不一定相同，那我們能不能找到一堆物品其總重量剛好符合背包所能裝載的重量。它的數學描述是指給定一個自然數數列 $B = \{b_1, b_2, \ldots, b_n\}$ 及一數 S，是否存在一子數列 $B' \subseteq B$，其中 $B' = (b'_1, \ldots, b'_m)$，使得 $\sum_{i=1}^{m} b'_i = S$ ？

背包難題已經被証實是一個 NP-Complete 問題，並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，自從 Diffie 及 Hellman[12]向世人介紹了公開金鑰密碼的概念之後，其中較著名的為 Merkle-Hellman[13]背包密碼系統。

但這種密碼系統被發現是不安全的，因為這種密碼系統中的「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[14]，之後陸陸續續又有許多學者提出攻擊方式，其中較為特別的是一位 Brickell[15]的學者所提出的低密度攻擊方式，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，就有可能被猜出來，而背包密碼系統也可能因此瓦解。背包密碼系統之所以不安全的原因是在設計系統時，多以易解背包難題之方式設計序列，然後在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，仍要面臨低密度攻擊的問題，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[16]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(例：低密度攻擊等)及密鑰恢復攻擊。「基於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。

2.3.3 整合式存取控制系統

曹偉駿等人[17]也利用 Hwang、Shao 與 Wang 提出「將一整數分解成質因數的乘積是唯一」的特性做為服務的存取值，並植基於「ECC 的自我認證公開金鑰密碼系統」與角色為基礎的存取控制方式，建構出具有高效率的整合式存取控制系統，儘管仍有不少學者研究存取控制方法，惟僅曹偉駿以跨服務中心為探討研究，但其方法尚有改進空間，為本研究比較對象，特列入文獻探討。

另外，由於存取規則的制定與存取權限的建立在每個獨立的內部網路都不盡相同，這也使得網路服務環境中的存取控制會產生主體或受體在不同網路服務站台(Web Site)中具有不同的定義，故提出角色轉換的做法，如表 1[18]，才能使得跨網域的使用者取得相對應的服務，系統流程分述如後：

表 1.角色轉換表

CA_Role	角色值	Web_Role
CA1	2	W3
CA2	3	W2
CA3	5	W1
CA4	7	W4

2.3.3.1 註冊階段

在本階段中，註冊的目的是在透過橢圓曲線密碼系統為基礎之自我認證公開金鑰密碼系統以取得公鑰及私鑰，如圖 3[17]。

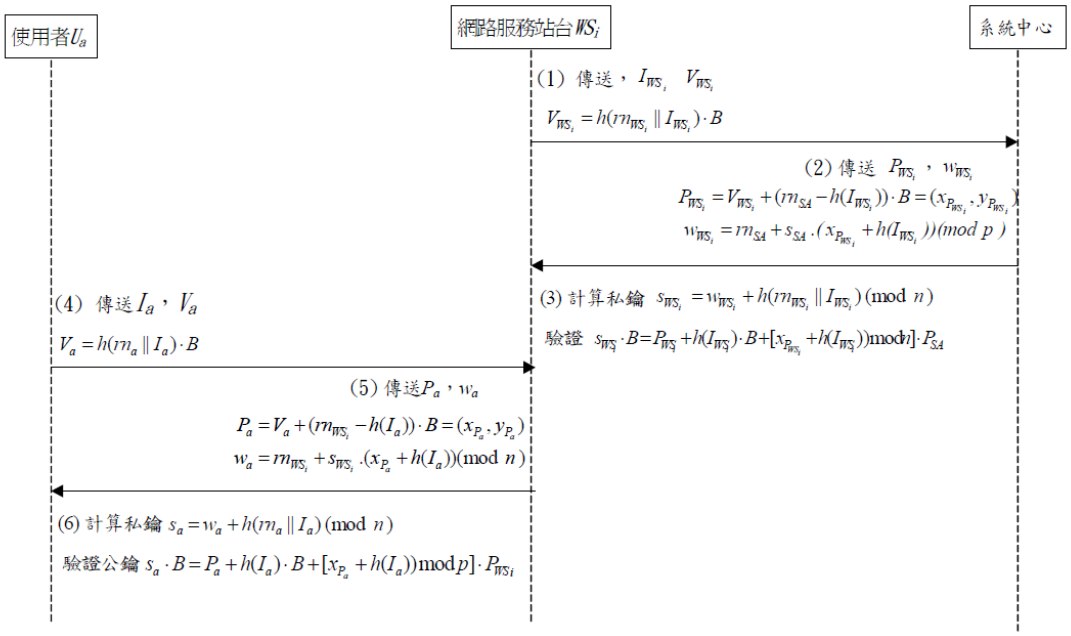


圖 3.註冊階段循序圖。

2.3.3.2 登入與驗證階段

使用者，如圖 4[17]。

身分驗證主要目的是在確認使用者為一合法

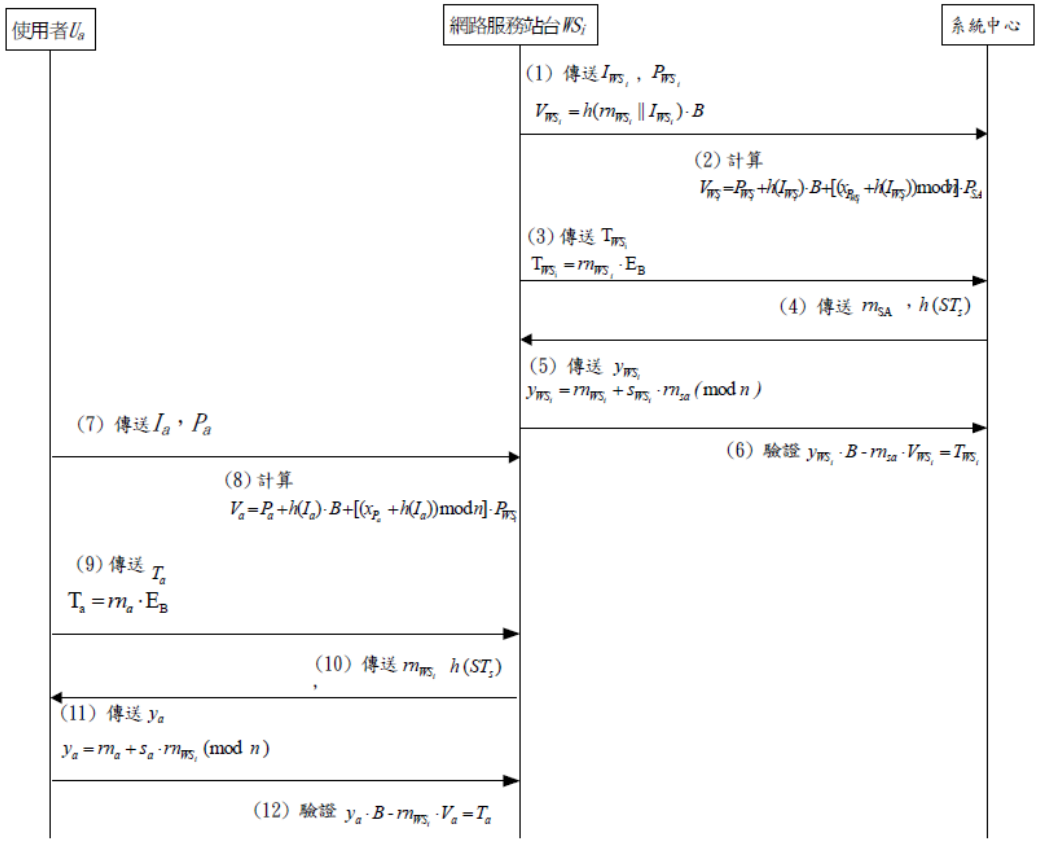


圖 4.登入與驗證階段循序圖。

2.3.3.3 資料加/解密階段

說明使用者與站台之間傳送與接收資料時如何進行加密及解密，如圖 5[17]。

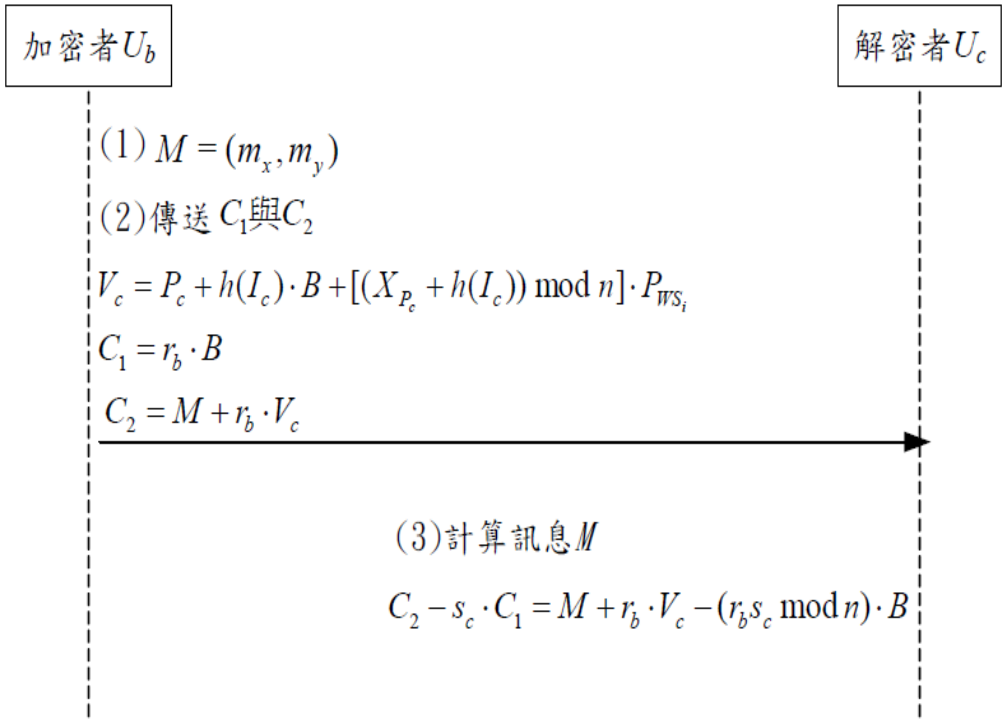


圖 5.資料加/解密階段循序圖。

曹偉駿等人提出此方法雖具跨網域架構，但仍必須透過角色伺服器執行角色值轉換。此外，利用「將一整數分解成質因數的乘積是唯一」的特性做為服務的存取值屬於易解背包序列之設計，仍然會面臨到低密度攻擊之風險。

三、研究方法

各軍種使用者在使用雲端服務，如郵件系統、AD 帳戶管理、檔案伺服器等，均僅能存取原軍種服務中心資源，若遇跨軍種專案編組或資源須跨服務平台存取，則必須面臨資源受限問題，以救災資源為例，若遇風災來臨前，各級部隊需超前部署至各災區，常面臨氣象資源不足，而災害來臨後，災區第一線圖資狀況掌握無法即時更新等問題。惟本研究主要貢獻仍於未來國軍走向雲端化後，針對跨雲端服務中心在存取控制上之運用以及資料傳遞在安全性上面臨的問題，並透過本方法(跨服務中心)與傳統存取控制之分析比較，期能提出適用於跨雲端服務中心之存取控制方法，增加服務提供之彈性及安全性。本方法透過動態的特性，使用者依授權服務使用及存取權限變更，且透過服務中心之間相互認證，可更快更安全的讓使用者取得所須雲端服務中心資源，增加服務中心之使用彈性，而管理端僅須管理雲端服務中心合法性，降低管理風險。本章將針對所提方法之運作流程及系統架構分別說明：

3.1 本系統整體運作流程架構及參數表

系統的整體運作流程如圖 6 所示，系統參數表如表 2 所示：

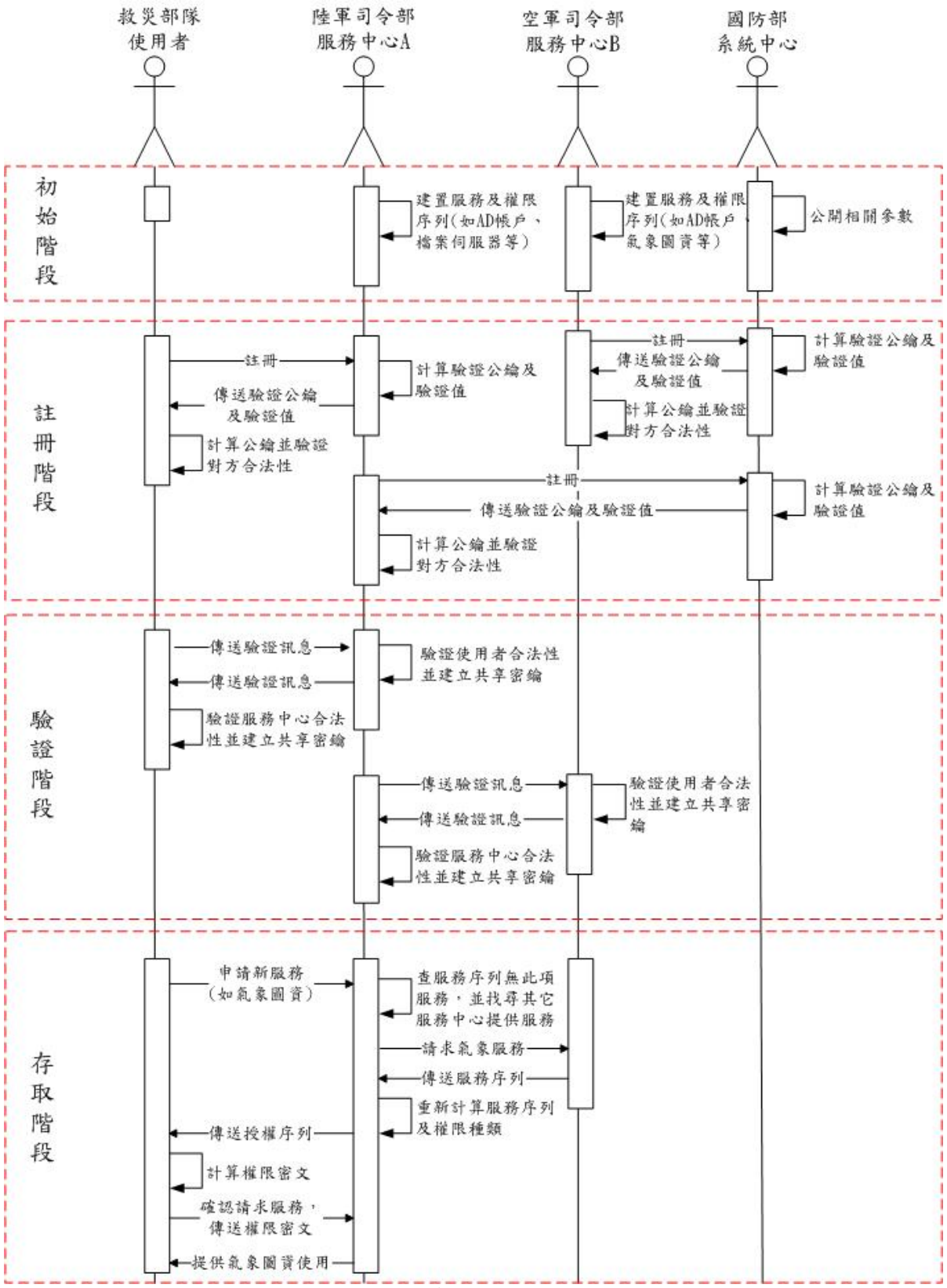

救災部隊
使用者
陸軍司令部
服務中心A
空軍司令部
服務中心B
國防部
系統中心
初始階段
建置服務及權限序列(如AD帳戶、檔案伺服器等)
建置服務及權限序列(如AD帳戶、氣象圖資等)
公開相關參數
註冊階段
註冊
計算驗證公鑰及驗證值
傳送驗證公鑰及驗證值
計算公鑰並驗證對方合法性
驗證階段
傳送驗證訊息
驗證使用者合法性並建立共享密鑰
驗證服務中心合法性並建立共享密鑰
存取階段
申請新服務(如氣象圖資)
查服務序列無此項服務，並找尋其它服務中心提供服務
請求氣象服務
傳送服務序列
重新計算服務序列及權限種類
傳送授權序列
計算權限密文
確認請求服務，傳送權限密文
提供氣象圖資使用

圖 6.系統架構圖。

表 2.系統符號說明表

項次	符號	說明
1	KGC	國防部系統中心
2	U_A	使用者
3	W_{S_i}、$W_{S_i}^*$	陸軍服務中心 A 及空軍服務中心 B
4	$E(F_q)$	橢圓曲線
5	A	控管服務之序列
6	t_A	授權服務種類之列
7	B	服務使用權限序列
8	t_B	授權服務權限種類序列
9	V_A	U_A的簽名檔
10	W_A	U_A的簽章
11	d_A、d_S、d_{S^*}	U_A及W_{S_i}、$W_{S_i}^*$選取的隨機參數
12	$PK_{W_{Si}}$、$PK_{W_{Si}^*}$	系統中心產生給W_{S_i}及$W_{S_i}^*$的驗證公鑰
13	S_S、S_{S^*}	W_{S_i}及$W_{S_i}^*$產生的公開金鑰
14	Sk_S、 Sk_{S^*}	W_{S_i}及$W_{S_i}^*$產生的私密金鑰
15	$K_{(S,S^*)}$	W_{S_i}及$W_{S_i}^*$之共享金鑰
16	k_A、k_A'	U_A隨機的一個參數
17	Af、 At	服務使用權限值及存取權限種類值
18	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
19	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

3.2 系統初始階段

系統初始階段含系統建置階段、軍種雲端服務中心$(W_{S_i}、W_{S_i}^*)$建置服務及權限序列，分述如後：

3.2.1 國防部系統中心(KGC)建置階段，程序如下：

(1)步驟 1：
由系統中心(KGC)在有限域F_q上選取一條安全的橢圓曲線(q 為一個 224bits 以上之大質數)，在 $E(F_q)$上選一階數(order)為 n 的基點 G，使 $nG=O$，其中 O 為此橢圓曲線之無窮遠點。
(2)步驟 2：
KGC 選擇單向無碰撞雜湊函數$h(\,)$及私鑰sk_{KGC}，並計算公開金鑰PK_{KGC}。

$$PK_{KGC} = sk_{KGC}G \tag{1}$$

(3)步驟 3：
KGC 公開 $E(F_q)$、G、n、$h(\,)$。

3.2.2 軍種雲端服務中心$(W_{S_i}、W_{S_i}^*)$建置服務及權限序列，程序如下：

(1)步驟 1：
各軍種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$U = (u_1, u_2 \dots, u_n)$，且$u_i$均為正整數。

計算向量$V=(v_1,\ v_2\ldots,\ v_n)$，其中$v_i=u_i-2^{n-1},i=1,\ldots,n$。

隨機選取兩個質數g_n和f_n(須滿足$q>4g_nf_n$)，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。

$$g_n>\sum_{i=1}u_i\ ,\ f_n>2\max\{\sum_{v_i>0}v_i\ ,-\sum_{v_i>0}v_i\} \tag{2}$$

利用餘式定理求得服務序列
$A=(a_1,a_2,\ldots,a_n),0\le a_i\le g_nf_n-1$。

$$a_i\equiv u_i(\mathrm{mod}\ g_n),a_i\equiv v_i(\mathrm{mod}\ f_n),i=1,\cdots,n \tag{3}$$

以[0,1]分別代表是否允許使用者使用該服務。

$$t_A=(t_1,t_2,\cdots,t_n),t_n\in[0,1] \tag{4}$$

計算服務使用權限值

$$Af=\sum_{i=1}^{n}A\times t_A \tag{5}$$

(2)步驟 2：

各軍種服務中心$(W_{S_i}$、$W_{S_i}^*)$建立授權之服務存取權限種類序列。

隨機選取 m 維向量$U^*=(u_1^*,u_2^*\cdots,u_m^*)$，且$u_i^*$均為正整數。

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

隨機選取兩個質數g_m和f_m，須滿足$q>4g_mf_m+1$(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。

$$g_m>\sum_{i=1}^{m}u_i^*\ ,\ f_m>2\max\{\sum_{v_i^*>0}v_i^*\ ,-\sum_{v_i^*>0}v_i^*\} \tag{6}$$

使用中國餘式定理計算權限種類序列
$B=(b_1,b_2,\ldots,b_n),0\le b_i\le g_mf_m-1$。

$$b_i\equiv u_i^*(\mathrm{mod}g_m),b_i\equiv v_i^*(\mathrm{mod}f_m),i=1,\cdots,m \tag{7}$$

以[0,1]分別代表是否允許使用者使用該服務。

$$t_B=(t_1,t_2,\cdots,t_m),t_m\in[0,1] \tag{8}$$

計算授權服務之存取權限種類值。

$$A\ t\ =\sum_{i\ =\ 1}^{m}\ B\ \times\ t_{\ B} \tag{9}$$

(3)步驟 3：

各軍種服務中心$(W_{S_i}$、$W_{S_i}^*)$將服務序列 A 及存取權限種類序列 B 儲存於資料庫，俾利使用者查詢。

3.3 登入註冊階段

在登入階段，陸軍服務中心W_{si}向國防部認證中心註冊，且使用者 U_A 向陸軍服務中心W_{si}註冊，參與金鑰建置。

(1)步驟 1：

陸軍服務中心W_{si}以自己$ID_{W_{si}}$及隨機參數$d_{W_{si}}\in[2,n-2]$，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$V_{W_{si}}$傳給國防部系統中心。

$$V_{W_{si}}=h(d_{W_{si}}||ID_{W_{si}})G \tag{10}$$

(2)步驟 2：

國防部系統中心 KGC 選擇一隨機參數值$k_{W_{si}}\in[2,n-2]$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：

$$PK_{W_{si}}=\left[V_{W_{si}}+\left(k_{W_{si}}-h(ID_{W_{si}})\right)\right]G=(q_{ax},q_{ay}) \tag{11}$$

$$W_{W_{si}}=k_{W_{si}}+sk_{KGC}\left(q_{ax}+h(ID_{W_{si}})\right) \tag{12}$$

(3)步驟 3：

陸軍服務中心W_{si}利用系統中心 KGC 傳回之參數$(PK_{W_{si}},W_{W_{si}})$自己計算私鑰$sk_{W_{si}}$，並利用簽章$W_{W_{si}}$驗證公鑰$PK_{W_{si}}$的正確性，計算式如下：

$$sk_{W_{si}}=[W_{W_{si}}+h(d_{W_{si}}||ID_{W_{si}})] \tag{13}$$

證明式如下：

$$\because S_{W_{si}}=sk_{W_{si}}G \tag{14}$$

$$S_{W_{si}}=\left[k_{W_{si}}+sk_{KGC}\left(q_{ax}+h(ID_{W_{si}})\right)+h(d_{W_{si}}||ID_{W_{si}})\right]G \tag{15}$$

$$S_{W_{si}}=\left[k_{W_{si}}+sk_{KGC}\left(q_{ax}+h(ID_{W_{si}})\right)\right]G+h(d_{W_{si}}||ID_{W_{si}})G \tag{16}$$

$$\because PK_{KGC}=sk_{KGC} \tag{17}$$

$$S_{W_{si}}=[k_{W_{si}}+h(d_{W_{si}}||ID_{W_{si}})]G+\left[\left(q_{ax}+h(ID_{W_{si}})\right)\right]PK_{KGC} \tag{18}$$

$$\because V_{W_{si}}=h(d_{W_{si}}||ID_{W_{si}})G \tag{19}$$

$$\because PK_{W_{si}}=V_{W_{si}}+\left(k_{W_{si}}-h(ID_{W_{si}})\right)G \tag{20}$$

$$V_{W_{si}}=PK_{W_{si}}-\left(k_{W_{si}}-h(ID_{W_{si}})\right)G \tag{21}$$

$$S_{W_{si}}=k_{W_{si}}G+V_{W_{si}}+[(q_{ax})+h(ID_{W_{si}})]PK_{KGC} \tag{22}$$

$$S_{W_{si}} = PK_{W_{si}} + h(ID_{W_{si}})G + [(q_{ax}) + h(ID_{W_{si}})]PK_{KGC} \quad (23)$$

陸軍服務中心W_{si}與國防部系統中心進行註冊，一旦各軍種成員自認證中心完成註冊並取得自己的公鑰PK_n及簽章W_n後，則不需國防部認證中心於系統中執行身分認證工作，可憑認證中心核發的帳戶相關資料（ID_n、PK_n）與自行計算的S_n，進行相互身分認證。同樣的，使用者U_A亦對陸軍服務中心W_{si}完成註冊並取得屬於自己的公鑰及簽章。

3.4 驗證階段

陸軍服務中心W_{si}自系統中心取得合法認證身分後，可憑帳戶資料與空軍服務中心$W_{S_i}^*$進行相互身分驗證，產生共享秘鑰$K_{(S,S^*)}$前，陸軍服務中心W_{si}需與空軍服務中心$W_{S_i}^*$相互確認$(ID_{W_{si}}$、$S_{W_{si}}$、$PK_{W_{si}})$及$(ID_{W_{Si}^*}$、$S_{W_{Si}^*}$、$PK_{W_{Si}^*})$是否正確，驗證無誤後即可建立共享秘鑰$K_{(S,S^*)}$，驗證檢查式如下：

$$S'_{W_{si}} = PK_{W_{si}} + h(ID_{W_{si}})G + [(q_{ax}) + h(ID_{W_{si}})]PK_{KGC} \quad (24)$$

$$S'_{W_{si}} ?= S_{W_{si}} \quad (25)$$

同時$S_{W_{si}}$也可驗證之$S'_{W_{Si}^*} ?= S_{W_{Si}^*}$，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$K_{(S,S^*)}$。

$$K_{(S,S^*)} = Sk_{W_{si}} \times S_{W_{Si}^*} = Sk_{W_{si}^*} \times S_{W_{si}} \quad (26)$$

同樣的，使用者與其軍種服務中心利用此驗證過程建立共享秘鑰$K_{(A,S)}$。

3.5 存取階段

使用者U_A向陸軍服務中心(W_{si})提出跨服務使用申請，經服務中心之間相互認證後，由空軍服務中心$(W_{S_i}^*)$回傳申請之服務及權限序列至陸軍服務中心(W_{si})，使用者即可享有不同服務中心間之服務。

(1)步驟 1：

U_A向陸軍服務中心(W_{si})反應所需氣象圖資服務不在服務序列 A 內，進而提出跨服務申請，陸軍服務中心(W_{si})透過服務中心間之相互認證發現空軍服務中心$(W_{S_i}^*)$擁有該服務，請求將授權服務序列及服務存取權限種類序列回傳，並產生新的授權服務序列 A 及服務存取權限種類序列 B。

(2)步驟 2：

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。

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

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

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

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。

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

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

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

(3)步驟 3：

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，方程式(34) - (36)為 ECC 加密運算。

$$M = \left((A_f', A_t') + K_{(A,S)}\right) = (m_1, m_2) \quad (33)$$

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

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

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

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

(4)步驟 4：

使用者傳送權限密文C_{A_0}給陸軍服務中心(W_{si})。

(5)步驟 5：

陸軍服務中心(W_{si})接收到使用者傳送的權限密文C_{A_0}之後，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$K_{(A,S)}$，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，即可得到服務

使用權限及權限種類。

$$C_{g_n} = A_f^{'} \bmod g_n, 0 \le C_{g_n} \le g_n - 1 \quad (41)$$

$$C_{f_n} = A_f^{'} \bmod f_n, -\frac{C_{f_n}}{2} < C_{f_n} < \frac{C_{f_n}}{2} \quad (42)$$

$$\left(C_{g_n} - C_{f_n}\right)_2 = t_{U_A} = (t_1, t_2, \cdots, t_n), t_n \in [0,1] \quad (43)$$

$$C_{g_m} = A_t^{'} \bmod g_m, 0 \le C_{g_m} \le g_m - 1 \quad (44)$$

$$C_{f_m} = A_t^{'} \bmod f_m, -\frac{C_{f_m}}{2} < C_{f_m} < \frac{C_{f_m}}{2} \quad (45)$$

$$\left(C_{g_m} - C_{f_m}\right)_2 = t_{U_A}^* = (t_1, t_2, \cdots, t_n), t_n \in [0,1] \quad (46)$$

(6)步驟 6：
陸軍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。

四、系統模擬

本章將針對所提方法之系統架構，實際帶入數據進行系統實作，說明如下：

4.1 系統初始階段

系統初始階段含系統建置階段、軍種雲端服務中心$(W_{S_i}$、$W_{S_i}^*)$建置服務及權限序列，分述如後：

4.1.1 國防部系統中心(KGC)建置階段，程序如下：

(1)步驟 1：
系統中心(KGC)在有限域F_q上選取一條安全的橢圓曲線$(F_q): y^2 = x^3 + 2x + 6\ mod q$，選擇質數$q = 9013$，在$E(F_q)$上選一階數(order)為$n = 8908$的基點$G$=(1,3)，使得$8908G = O$，其中$O$為此橢圓曲線之無窮遠點。
(2)步驟 2：
KGC 選擇單向無碰撞雜湊函數$h(\,)$及私鑰$sk_{KGC} = 9$，並計算公開金鑰PK_{KGC}。

$$PK_{KGC} = sk_{KGC}G = 9(1,3) = (2074,6035)$$

(3)步驟 3：
公開$(F_q): y^2 + 2x + 6\ mod q$、$G$=(1,3)、n = 8908、$PK_{KGC} = (2074,6035)$、$h(\,)$。

4.1.2 軍種雲端服務中心$(W_{S_i}$、$W_{S_i}^*)$建置服務及權限序列，程序如下：

(1)步驟 1：
各軍種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 3 維向量$U = (9, 11, 6)$。
計算向量$V = (5, 9, 5)$。
隨機選取兩個質數$g_n = 29$和$f_n = 43$(須滿足$q > 4g_nf_n$)。
利用餘式定理求得服務序列
$A = (908,1084,116), 0 \le a_i \le g_nf_n - 1$。
(2)步驟 2：
各軍種服務中心$(W_{S_i}$、$W_{S_i}^*)$建立授權之服務存取權限種類序列。
隨機選取 6 維向量$U^* = (16,8,7,5,2,1)$。
計算向量$V^* = (-16,-8,-1,1,0,0)$。
隨機選取兩個質數$g_m = 37$和$f_m = 53$，須滿足$q > 4g_mf_m + 1$。
使用中國餘式定理計算權限種類序列
$B = (90,45,1006,1485,742,371), 0 \le b_i \le g_mf_m - 1$。
(3)步驟 3：
各軍種服務中心$(W_{S_i}$、$W_{S_i}^*)$將服務序列$A = (908,1084,116)$及存取權限種類序列$B = (90,45,1006,1485,742,371)$儲存於資料庫，俾利使用者查詢。

4.2 登入註冊階段

在登入階段，陸軍服務中心W_{si}向國防部認證中心註冊，且使用者U_A向陸軍服務中心W_{si}註冊，參與金鑰建置。
(1)步驟 1：
陸軍服務中心W_{si}以自己$ID_{W_{si}} = 123$及隨機參數$d_{W_{si}} = 432$透過單向無碰撞雜湊函數$h\left(d_{W_{si}} || ID_{W_{si}}\right) = 21$產生簽名檔$V_{W_{si}}$，並將$ID_{W_{si}}$與$V_{W_{si}}$傳給國防部系統中心。

$$V_{W_{si}} = h\left(d_{W_{si}} || ID_{W_{si}}\right)\mathrm{G} = 21(1,3) = (6070,7155)$$

(2)步驟 2：
國防部系統中心 KGC 選擇一隨機參數值$k_{W_{si}} = 31$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：

$$PK_{W_{si}} = (6070,7155) + 16(1,3)$$

$$= (6070,7155) + (5334,7556)$$

$$= (4072,6525) = (q_{ax}, q_{ay})$$

$$W_{W_{si}} = 31 + 9(4072 + 15) = 3681$$

(3)步驟 3：

陸軍服務中心W_{si}利用系統中心 KGC 傳回之參數$(PK_{W_{si}}, W_{W_{si}})$自己計算私鑰$sk_{W_{si}}$，並利用簽章$W_{W_{si}}$驗證公鑰$PK_{W_{si}}$的正確性，計算式如下：

$$sk_{W_{si}} = (36814 + 21) = 36835$$

證明式如下：

$$\because S_{W_{si}} = sk_{W_{si}}G = 36835G = (8224,7690)$$

$$S_{W_{si}} = (4072,6525) + 15(1,3) + [(4072 + 15)](2074,6035)$$

$$S_{W_{si}} = (4072,6525) + (6316,4684) + 4087(2074,6035)$$

$$S_{W_{si}} = (5628,5821) + 4087(2074,6035)$$

$$S_{W_{si}} = (5628,5821) + (6040,2038)$$

$$S_{W_{si}} = (8224,7690) = S'_{W_{si}}$$

4.3 驗證階段

陸軍服務中心W_{si}自系統中心取得合法認證身分後，可憑帳戶資料與空軍服務中心$W^*_{S_i}$進行相互身分驗證，產生共享秘鑰$K_{(S,S^*)}$前，陸軍服務中心W_{si}需與空軍服務中心$W^*_{S_i}$相互確認$(ID_{W_{si}}、 S_{W_{si}}、PK_{W_{si}})$ 及$(ID_{W^*_{Si}}、 S_{W^*_{Si}}、PK_{W^*_{Si}})$是否正確，驗證無誤後即可建立共享秘鑰$K_{(S,S^*)}$：

$$K_{(S,S^*)} = Sk_{W_{si}} \times S_{W^*_{Si}} = Sk_{W^*_{Si}} \times S_{W_{si}}$$

$$K_{(S,S^*)} = 36835 \times (477,4506) = 44360 \times (8224,7690)$$

$$K_{(S,S^*)} = 1203 \times (477,4506) = 8728 \times (8224,7690)$$

$$K_{(S,S^*)} = (196,3303)$$

同樣的，使用者與其軍種服務中心利用此驗證過程建立共享秘鑰$K_{(A,S)}$。

4.4 存取階段

使用者U_A向陸軍服務中心(W_{si})提出跨服務使用申請，經服務中心之間相互認證後，由空軍服務中心$(W^*_{S_i})$回傳申請之服務及權限序列至陸軍服務中心(W_{si})，使用者即可享有不同服務中心間之服務。

(1)步驟 1：

U_A向陸軍服務中心(W_{si})反應所需氣象圖資服務不在服務序列 A 內，進而提出跨服務申請，陸軍服務中心(W_{si})透過服務中心間之相互認證發現空軍服務中心$(W^*_{S_i})$擁有該服務，請求將授權服務序列及服務存取權限種類序列回傳，並產生新的授權服務序列 A 及服務存取權限種類序列 B。

(2)步驟 2：

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。

$$A = (908,1084,1166), 0 \le a_i \le g_n f_n - 1$$

$$t_{U_A} = (1,1,1), t_n \in [0,1]$$

$$A'f = (908\times1)+(1084\times1)+(1166\times1) = 3158$$

計算權限種類值。

$$B = (90,45,1006,1485,742,371), 0 \le b_i \le g_m f_m - 1$$

$$t^*_{U_A} = (1,1,1,0,1,0), t_m \in [0,1]$$

$$A't = (90\times1)+(45\times1)+(1006\times1)+(742\times1) = 1883$$

(3)步驟 3：

U_A隨機擇一參數$k'_A = 502$，令權限明文成為點訊息，並計算使用者權限密文。

$$M = \big((3158,1883) + (678,3945)\big) = (5513,3673)$$

$$C_{A_1} = 502(1,3) = (3493,719)$$

$$Y_A = 502(8224,7690) = (3423,443) = (y_{A_1}, y_{A_2})$$

$$C_{A_2} = (C_{21}, C_{22}) = (3423 \times 5513 \bmod 9013, 443 \times 3673 \bmod 9013) = (6790,4799)$$

$$C_{A_0} = \big(C_{A_1}, C_{A_2}\big) = ((3493,719),(6790,4799))$$

(4)步驟 4：

使用者傳送權限密文$C_{A_0} = ((3493,719),(6790,4799))$給陸軍服務中心。

(5)步驟 5：

陸軍服務中心(W_{si})接收到使用者傳送的權限密文C_{A_0}之後，解開C_{A_0}內容。

服務中心以私鑰 $Sk_S = 36835$計算Z值。

$$Z = Sk_S \times C_{A_1} = 36835(3493,719) = 1203(3493,719) = (3423443) = (Z_1, Z_2)$$

服務中心利用共享秘鑰$K_{(A,S)} = (678,3945)$，即可得到服務使用權限及權限種類值。

$$M = \left(6790 \times 3423^{-1} \bmod 9013, 4799 \times 443^{-1} \bmod 9013\right)$$
$$M = (6790 \times 1672 \bmod 9013, 4799 \times 5066 \bmod 9013)$$
$$M = (5513, 3673) = (m_1, m_2)$$

$$(A'f, A't) = (5513, 3673) - (678, 3945)$$
$$(A'f, A't) = (5513, 3673) + (678, -3945)$$
$$(A'f, A't) = (5513, 3673) + (678, 5068)$$
$$(A'f, A't) = (3158, 1883)$$

依服務使用權限及權限種類值，即可得到服務使用權限及權限種類。

$$C_{g_n} = 3158 \bmod 29 = 26$$
$$C_{f_n} = 3158 \bmod 43 = 19$$
$$(C_{g_n} - C_{f_n})_2 = (26 - 19)_2 = (1,1,1)_2$$
$$C_{g_m} = 1883 \bmod 37 = 33$$
$$C_{f_m} = 1883 \bmod 53 = -25$$
$$(33 - (-25))_2 = (58)_2 = (1,1,1,0,1,0)_2$$

(6)步驟 6：
陸軍服務中心依服務使用權限值$t_{U_A} = (1,1,1)$，判定使用者對哪些服務具使用權限，並依權限種類值$t^*_{U_A} = (1,1,1,0,1,0)$判定使用者對授權服務具有哪些存取權限種類。

五、安全性及效益分析

目前研究結果係根據 ISO 組織所提出資訊系統安全性管理需求：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；另依據本研究內容，可達到身分驗證、存取控制等額外之安全需求；此外，參酌文獻[18]所提之運算量，時間複雜度運算相互關係表如表 3，本研究與曹偉駿「整合式系統」在時間複雜度上相比較，成果如表 4，相關效益分析的說明如後：

5.1 機密性(Confidentiality)

機密性是指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。本系統中密文傳輸使用了橢圓曲線公開金鑰之加密方法，管理者以橢圓曲線點加法，編碼如(33)式，將使用者存取權限予以編碼。破譯者若想解開這些資訊，將面臨橢圓曲線離散對數難題，需先經由破解(34)、(35)與(36)式，再從(33)式中設法得知使用者服務使用及權限種類值$(A'_f、A'_t)$與取得雙方共享金鑰；儘管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$(A'_f、A'_t)$，仍然會再面臨到隨機背包難題，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，這類的問題已經被証實是一個 NP-Complete 問題，無法在多項式時間內解決。

5.2 完整性(Integrity)

完整性是指對資料之精確與完整安全保證的特性。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資訊，否則傳送至系統中心之存取權限是無法被更改的。編碼如(10)式將自己的簽名檔傳送給對方(系統中心)，對方(系統中心)也將使用者身分訊息進行雜湊運算，再結合使用者簽名檔透過(11)式，運算並回傳，若第三方想要竄改或偽冒使用者簽章而不被發現，則他將面對破解單向雜湊函數(One-Way Hash Function, OWHF)及橢圓曲線離散對數難題；假若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，將面對破解橢圓曲線離散對數難題，否則傳送至服務中心之服務使用及權限是無法被偽冒或更改的。

5.3 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。在系統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如(33)式。在共享秘鑰內含雙方傳給認證中心之公鑰。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，其中私鑰是由使用者利用身分資料參與金鑰建置，已經將個人資訊隱含在內如(13)式，使用者無法否定提出服務請求或使用過該服務。

5.4 身分認證(Authentication)

身分認證指的是可以提供線上另一使用者的確認性服務，也就是本方法透過自我認證機制達到可攜性的效益，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，日後當雙方需要進行資料傳輸時，可以利用彼此的身分資料及驗證公鑰去驗證雙方是否為合法使用者如(23)式，不需再透過系統中心做保證與協調。

表 3.時間複雜度運算之相互關係參考表

符號	定義	相互關係
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	$\approx 0.12\ T_{MUL}$
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	$\approx 1T_{MUL}$

5.5 存取控制(Access Control)

存取安全性指的是存取權限值管理上的安全。本研究提出利用序列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，且該序列僅以 1 或 0 來表示是否具該物件之使用及相關權限，再結合隨機背包密碼系統求得服務使用及權限種類值，做為判斷服務請求及存取權限範圍，這種方式可以讓服務提供者在使用者所註冊的合理授權範圍，提供使用者服務使用及權限選擇之彈性。

表 4.本研究時間複雜度比較表

演算法	整合式存取控制系統演算法(曹偉駿，2010)		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	$3T_{ECADD} + 2t_h + 1T_{ECMUL}$	$\approx 31.36T_{MUL}$	$3T_{ECADD} + 2t_h$	$\approx 2.36T_{MUL}$
加密運算	$4T_{ADD} + 2t_h + 4T_{MUL}$	$\approx 6T_{MUL}$	$1T_{ECADD}$	$\approx 0.12T_{MUL}$
解密運算	$3T_{ADD} + 3T_{MUL}$	$\approx 3T_{MUL}$	$2T_{ECMUL}$	$\approx 58T_{MUL}$
驗證運算	$4T_{ECMUL}$	$\approx 116T_{MUL}$	$3T_{ECADD} + 2t_h$	$\approx 2.36T_{MUL}$
Total	$\approx 156.36T_{MUL}$		$\approx 62.84T_{MUL}$	

六、結論

適逢國軍組織結構改革，作業流程 e 化，以及未來戰爭型態改變等，國防雲端運算應用乃時勢所趨，未來國軍須思考如何有效資源整合，打破原先軍種界線與藩籬的觀念，並在資訊安全前提下，達到跨雲端服務機制，另亦須同步考量組織再造及資訊化議題，以使國防部系統中心及各軍種服務中心能有效整合資源、發展新型態綜合型服務。透過本研究提出軍種跨服務存取控制及相互認證機制，增加雲端服務的使用彈性及安全性，將可作為國軍在建置雲端運算環境的參考。本研究預期貢獻如下：

(1)系統後端可以隨時根據權限的變動提供使用者服務，增加服務的彈性以及使用者的方便，且授權服務及權限已植基於隨機背包之難題將資訊隱藏，攻擊者無法得知服務及權限內容。

(2)透過存取控制有效率的在雲端環境下跨不同組織架構作個人服務存取，透過加密及監控管理，讓使用者安全使用，是最佳實務與安全工具的應用。

(3)建置可離線作業之身分認證機制，避免服務中斷。

(4)以橢圓曲線密碼系統執行權限密文加密，

在同樣的密鑰長度下，擁有更高安全性，更適用於雲端環境下。

參考文獻

[1] 陳瀅，王慶波，金淶，趙陽，何樂，鄒志樂，吳玉會，楊林，“雲端策略─雲端運算與虛擬化技術”，天下雜誌，第 15-18 頁，2010。

[2] 蘇品長，葉昱宗，王博彥，“跨服務平台之雲端運算探討”，2014 電子商務與數位生活研討會論文集，第 292-306 頁，2014。

[3] 朱近之主編，智慧的雲端運算-成就物聯網的未來基石，博碩文化，第 37-45 頁，2010。

[4] 蔡一郎，“雲端運算與雲端安全架構”，資訊安全通訊，第 16 卷，第 4 期，第 84-93 頁，2010。

[5] NIST，“TheNIST Definition of Cloud Computing”，下載於 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (2015 年 1 月 25 日)，2010。

[6] 游舒帆，“三種雲端服務”，下載於 http://www.dotblogs.com.tw/jimmyyu/archive/2009/12/03/12275.aspx (2014 年 6 月 24 日)，2009。

[7] 蘇品長，陳文彬，“適用於雲端環境下之動態服務存取方法”，國防管理學報，第 33 卷，第 2 期，第 1-14 頁，2012。

[8] Koblitz, N.,“Elliptic Curve Cryptosystems”, Mathematics of Computation American Mathematical Society, pp.203-209,1987.

[9] Miller, V. S.,“Use of Ellitic Curve in Cryptography”, Advance in Cryptography-Crypto, New York,Spring-Verlag, pp.417-426,1985.

[10] ElGamal, T.,“A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”, IEEE Trans.Information Theory,Vol. IT-31,No. 4, pp.469-472,1985.

[11] Menezes, A., and Vanstone, S.,“Elliptic Curve Cryptosystems and Their Implementation”, Journal of Cryptology, pp.209-224,1993.

[12] Diffie, W., and Hellman, M.E.,“New Directions in Cryptography”, IEEE Transactions on Information Theory, Vol. IT-22,No. 6, pp.644-654,1976.

[13] Merkle, R.C.,and Hellman, M., “Hiding Information and Signatures in Trapdoor Knapsacks”, IEEE Transactions on Information Theory, Vol. IT-24,No. 5, pp.525-530, 1978.

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

[15] Brickell, E.F., “Breaking Iterated Knapsacks”, Advances in Cryptology-Crypto’84, Springer-Verlag, pp.342-358, 1984.

[16] 王保倉，韋永壯，胡予濮，“基於隨機背包的公鑰密碼”，電子與信息學報，第 32 卷，第 7 期，第 1580-1584 頁，2010。

[17] 曹偉駿，黃美治，“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，第 159-182 頁，2010。

[18] Wang, R.C., “A Web Metering Scheme for Fair Advertisement Transaction,” InternationalJournal ofSecurityand its Application, Vol. IT-2,No. 4, pp.49-55,2008.