強化國軍雲端服務存取權限機制之設計

蘇品長　黃琮仁　蘇泰昌*

國防大學資訊管理學系

論文編號：NM43-01-06

來稿 2022 年 2 月 24 日→第一次修訂 2022 年 3 月 8 日→第二次修訂 2022 年 3 月 30 日→

同意刊登 2022 年 4 月 13 日

摘要

隨著科技日新月異，雲端空間之使用已進入普及的時代，綜觀民間企業及政府機關均有使用雲端空間功能提供客戶服務或是提供內部員工快速取得所需資料。國軍為達資訊快速傳遞及系統統一管理，故亦須使用雲端空間，惟現行國軍在使用者管理上，僅使用 AD 帳號及密碼的認證方式來登入各項系統，若其帳密遭竊將有機敏洩漏疑慮。本研究將基於橢圓曲線密碼系統、隨機背包密碼系統及結合智慧卡，利用相比 RSA 加密演算法擁有較小的密鑰長度且可達相同安全性的橢圓曲線密鑰與隨機背包密碼系統運算效能快，來強化國軍雲端服務系統的資訊安全及處理速度。

關鍵詞：雲端架構、身分認證，混合式金鑰系統

*通訊作者：蘇泰昌 email: believe50405@gmail.com

The Enhancement of Information Security for the Access Authority of Military Cloud System

Su, Pin-Chang Huang, Cong-Ren Su, Tai-Chang *

Department of Information Management, National Defense University.

Abstract

With the rapid development of technology, the application of cloud space had already entered the general era. More and more private enterprises and government agencies had utilized the cloud space to provide services for their customers or rapidly information acquisition for their employees. To achieve rapid information transmission and system unified management, it is necessary for the National Army to implement cloud space systems. However, only the Active Directory (AD) account and password were used in current National Army user management for the authentication to enter various systems. Therefore, there will be a risk of sensitive leakage if the accounts were been stolen. In this study, the information security and process speed of the cloud space service system of the Nation Army will be enhanced based on the Elliptic Curve Cryptography (ECC), random backpack cryptography system and combined with smart cards, taking the advantages of an elliptical curve key with a smaller key length compared to the RSA encryption algorithm and achieving the same security and random backpack cryptography system operation.

Keywords: Cloud Architecture, Identity Authentication, Hybrid Cryptosystem System.

* Corresponding Author Email: believe50405@gmail.com

一、前言

雲端時代的到來，影響了我們對 IT 基礎設施管理的思維方式，舉例來說，以軟體服務為基礎的供應商（Service Provider, SP）現在可以透過硬體平台外包方式，發展應用程式、系統或平台等雲端服務；對於使用者來說，不再需要去擔心網路或系統的資源是否充足，基礎設施是否能夠符合需求等問題，只需要關心真正需要的服務是那些，並透過終端設備連接上網路即可取得所需的服務。

綜觀各國軍隊講求陸、海、空三軍聯合作戰，隨著科技進步、網路及航太發展快速，各軍之間亦仰賴戰情資訊同步掌握，方能達到資訊同步、協同作戰之目的，除了聯合作戰，資訊戰亦已成為軍事發展的重要環節，俄國於 2017 年首次承認組建第一支網軍，俄國上議院國防與安全委員會主席受訪時表示，資訊戰部隊主要是保護俄國的數據系統不受敵人攻擊，不會向國外發動任何網路攻擊，美國也於同年宣布將美軍網路司令部升級為最高級別的聯合作戰司令部，其重點強調，網路司令部將進一步強化美國的網路安全，也將加強與盟邦的合作，對全球網路安全威脅做出快速反應（王子承，2017），中共在 2019 年發布的報告中談到，已將「網絡安全」與核武、導彈及太空等傳統軍事項目並列，並以相當篇幅論述網路安全面臨的威脅及後續發展規劃，其內容除證實相關國家的警訊外，更符合中共國家主席習近平所提出「沒有網絡安全，就沒有國家安全」的指示（劉嘉偉與張家瑛，2021，轉引自中共國防部，2019 與中共新聞網，2018）；但凡可運用電腦及使用網路連線之地點，都有可能成為敵方從事網路攻擊的目標，一旦網路遭受攻擊而癱瘓，將使整個國家受到極大的危害，因此，在面對軍事強國大量運用網路科技的威脅下，如何確保軍隊機敏資訊不外洩、特定資訊如何讓特定人員安全的使用等網際網路安全工作，將成為我軍發展科技作戰時必須重視的問題。

考量我國國軍雲端整合服務及運用上傳遞的大多為機敏情資，為防止資訊傳遞遭受非法存取或惡意存取等行為，並且在各軍種任務屬性不同所需存取雲端中資訊服務，故在系統建置上需要加速資料傳遞及資訊同步並設計更安全的身分認證機制，且必須為不同任務屬性使用者設定不同資料存取權限；因此，本研究所提方法係運用橢圓曲線密碼系統（Elliptic Curve Cryptosystem, ECC）演算法加上改良式隨機背包密碼系統（Random Knapsacks Cryptosystem, RKC）強化系統身分認證及資料交換方式，設計擁有處理時效快、安全性較高且彈性之演算法，做為依不同需求服務之身分驗證及存取權限控制方法，並結合國軍自行研發智慧卡（Smart Card）及一次性密碼的認證機制加強資料傳輸時的安全性，使各軍種合法認證使用者可自行依實際所需向國軍雲端服務中心提出功能使用服務及權限變動，亦可於臨時性任務需求時啟用相對應功能服務並獲取相關資訊。且在國軍雲端後端管理伺服器僅儲存依合法使用者需求所產生之功能服務及權限種類代數，如遭有心人士擷取，亦無法得知授權之功能服務及權限，符合資訊安全所需之管控與資料傳輸存取需求，加上橢圓曲線密碼加解密速度快等優點，期望達成下列目的：

- 設計動態修改權限存取控制方法，以降低雲端服務伺服器因權限集中控管之負擔，增進服務之即時性及國軍分層管制需求，且當使用者與雲端服務系統伺服器間建立認證後，可將所授權之任務功能及使用權適時調整，以提升運用彈性。
- 系統管理者僅存放公開之權限序列及加密保護之權限值，即使攻擊者獲取相關權限值，亦將面臨密碼解譯難題，無法在短時間內完成破解，且可避免服務提供者保留使用者相關參數資料。
- 不同使用者在資訊傳遞及資料交換時，均須透過存取權限認證機制後才可進行，除可依照軍種任務特性分類提高安全性外，透過高效率的運算，亦可加速存取權限認證程序。

二、文獻探討

本章分類整理、歸納分析與本研究相關的文獻，首先概述國軍跨軍種資料交換暨雲端架構進行介紹，接著針對雲端運算安全、身分認證機制及密碼學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 國軍跨軍種資料交換暨雲端架構

國軍跨軍種資料交換及雲端架構可概分為現行及未來推展進行說明，以現行雲端架構（如圖 1）來說，在雲端上使用之系統由各軍種機房自行維護，目前較為廣泛使用在公文處理系統、人事管理及門禁休請假系統。前述相關系統雖已使用個人帳密及智慧卡執行，在資料傳遞上仍是以明文方式進行傳輸，有心人士仍可駭進主服務中心端竊取或破壞相關資訊，影響資訊安全，而資料交換則因考量洩密風險尚無規劃軍種間使用雲端資料交換，各軍種僅開放單位間網域磁碟使用。

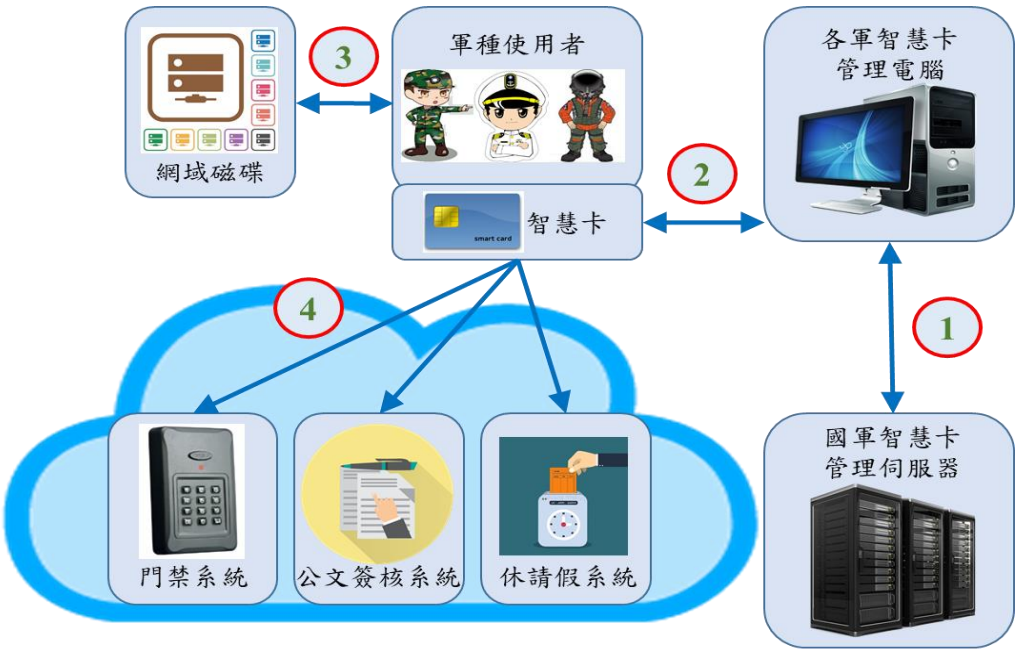

圖 1　國軍資料交換暨雲端架構示意圖

未來隨著科技蓬勃發展，作戰型態轉變，平時如何有效掌握各軍戰備整備情況，戰時如何快速提供各軍即時敵情、迅速與友軍共享部隊資訊將是國軍首重的課題，以現行營門管制為例，舊有的門禁管制主要區分為紙本管制及單點門禁系統，前者須簽奉營區權責長官才能入營，後者則是透過單位門禁系統管制入營，但各單位間使用的系統無法互通，即進入不同營區需有不同智慧卡導致個人與單位管理不易；國防部遂規劃推動全軍雲端整合運用，取代以往資料傳遞模式，並統一全軍門禁雲（如圖 2），往後只需雲端認證身分即可透過同一張智慧卡赴全軍各陣地執行公務，有效減少紙本作業，而門禁休請假及公文管理雲的統一只是其中的環節，重要的是建置一龐大的雲端存儲空間，提供全軍同仁使用及資料交換，這樣的措施不只縮短了軍種間資料傳遞及分享的時效，讓跨軍種公務協調更有效率，亦可使上層管理單位可同時快速傳達重要命令給不同單位，然而在新架構下，使用者的存取權限及資料傳遞上具有安全性上的疑慮，因此本研究便是在此架構下提出改良，以強化其安全性。

圖 2　國軍未來全軍雲端整合架構示意圖

2.2 雲端運算存取權限與安全

依據 NIST 的定義（Mell and Grance, 2011），雲端運算是一個模式，能隨時依照需求且便利的透過網路存取設定好的共享運算資源池（如網路、伺服器、儲存裝置、應用程式與各種服務），可以最少的管理工作或服務供應商互動，進行快速配置和發佈，強調雲端運算能按照使用者的需求，進行資源的靈活調配。這種雲端模型提升了服務可用性，可分為五個基本特徵（隨需自助服務、可隨時隨地存取網路、共享資源池、快速彈性與可量測得服務）、三個服務模式（架構即服務 IaaS、平台即服務 PaaS 與軟體即服務 SaaS）及四種佈署模型（私有雲端、社群雲端、公用雲端與混合雲端）。

在存取權限方面，現有知名的雲端運算平台包含 Eucalyptus、OpenStack 及 OpenNebula，將重點介紹這些平台在身分管理上的服務，Eucalyptus 是一種開源私有云軟件，用於構建與 Amazon Web Service（AWS）API 兼容的計算、網絡和存儲的私有或混合雲資源，其預設將所有身份存儲在本地雲端控制器（CLC）數據庫中 （Eucalyptus Identity and Access Management IAM, 2012），身份數據也可以從 LDAP 或 AD 中存取，然而在 2017 年發現一些未知功能的使用會使其機密性、完整性和可用性受到影響（Hewlett Packard Enterprise Development, 2017）；OpenStack 是一個開源雲計算項目，自 2010 年發布以來迅速發展（Kumar et al., 2014），其預設身份管理系統是 Keystone，現有的 Keystone 是集中式的，所有用戶都需要在其數據庫中註冊，由 OpenStack 管理員手動或通過從企業數據庫批量加載，然後再使用訪問任何服務，這種設計在使用上有諸多限制且在 2017 年也有發現其安全漏洞（Abdulla, N., & Erçelebi, E. ,2017）；OpenNebula 於 2005 年成立，許多企業在其基於 VMware 上用作開放的雲虛擬化基礎架構，從而實現高度可擴展的託管環境，OpenNebula 包括一個完整的用戶和群組管理系統，通常存取透過內部的用戶帳號密碼進行認證，但也可透過外部身份驗證驅動程序，但在網路性能上遠不及前二者，容易導致網路中斷問題（Brummett et al. 2015）。

雲端安全聯盟（Cloud Security Alliance, CSA）於 2013 年發表的文章中指出，雲端運算服務中最常見的安全威脅，包括資料洩漏、資料遺失、帳號詐騙或服務劫持、不安全的軟體介面、阻絕服務攻擊、內部員工的惡意行為、雲端服務的濫用、審慎評鑑不足、共享技術的漏洞等 9 項（CSA, 2013）。面對上述的安全威脅，該聯盟早在 2011 年時便闡述雲端運算所面臨的資訊風險及其對應的安全性建議，並提出建構雲端運算安全架構的方法：以「雲端架構（Cloud Architecture）」、「雲端治理（Governing in the Cloud）」、

「雲端營運（Operating in the Cloud）」三部分為主，再細分成十四項安全領域進行評估，其中「第五項」安全領域「資訊管理與資料安全」：提出必須依照機密性、完整性、可用性，以及資料的生命週期，實施相對應的控制措施及「第十一項」安全領域「加密與金鑰管理」：加密與金鑰管理是雲端運算資料保護的核心機制，在雲端環境中，用戶不應依賴雲端供應商所提供的加密安全機制，應當在機敏性資料傳輸至雲端前，利用適當的加密機制（標準且高安全強度的演算法）或資安產品將資料加密，當資料從原先受到良好控制的環境（CSA, 2011）。

2.3 身分認證機制

身分認證途徑可看作存取控制（Access Control）為最需重視的一環，用戶端必須先與認證伺服器證明自己的身分，來獲得授權（Authorization），才有讀寫、執行及刪除等權限，以下介紹幾種常見的認證方式：

- 使用者帳號/密碼（Username and Password）：現行普遍的方法，由使用者先向伺服器註冊用戶帳號及密碼，登入時必須輸入正確的帳號及密碼，伺服器才會提供正確的資訊及服務。帳號及密碼是相對靜態的，除非使用者自行更改，否則將維持不變，而使用者為提高靜態密碼的安全性，將定期對密碼進行修改或增加密碼的難度，但此舉容易造成密碼不易紀錄，所以使用者使用容易記住的密碼或以明碼紀錄保存，易遭有心人士破解或外洩。因為密碼是靜態的數據，身分認證機制在使用方面非常簡單，且驗證過程中很容易被攔截及破解，從安全性上來講，已經無法滿足網際網路對於身分認證安全性的需求（黃建衛，2011）。
- 一次性密碼（One Time Password, OTP）：一種產生單次使用密碼的機制，由學者 Lamport（1981）首先提出，可以確保密碼不會被連續重複使用。當使用者輸入帳號，準備登入系統時，必須再鍵入顯示在此裝置螢幕上的密碼，由後端驗證系統進行核對，使用過後立即失效，若遭受重複使用亦無法獲得系統的存取，藉此保護系統所提供服務之安全性，也保護使用者身分不易因此遭受盜用。其原理是植入一把對稱式金鑰（Symmetric Key），再以時間、使用次數或輸入內容等參數為變動值，經由特定的加密演算法及雜湊函數運算，再將結果轉換成密碼。
- 智慧卡（Smart Card）：一種具運算能力、儲存功能及自我保護的硬體，使用時為證明持有人確實為該卡的授權使用者，必須鍵入預先設定的密碼，並與卡片內儲存的密碼驗證無誤後方能運作。智慧卡具有儲存功能，通常會在卡片上植入一把對稱式金鑰，當使用者完成密碼驗證後，卡片與伺服器會進行挑戰與回應的驗證機制。先由伺服器送數值到卡片並以內建的對稱式金鑰運算後，將密碼送回伺服器後，再以卡片對應的對稱式金鑰進行運算比對，以確認使用者的合法性。

2.4 密碼學理論

密碼學（Cryptography）既指秘密書寫、加密訊息、隱藏訊息內容的科學，同時也泛指與密碼有關的科學，其中當代密碼系統則應提供機密性、完整性、身分認證及不可否認性等四大功能（鄧安文，2018），而如何強化密碼系統的安全性，取決於演算法的強度、金鑰保護的機制及加密長度，在幾經許多密碼學家與研究學者的努力下，越來越多的加密演算法也漸漸被提出，在本研究中選擇使用橢圓曲線密碼學及隨機背包密碼系統加入機制演算法推導，其優勢概述如後：

橢圓曲線在代數學和幾何學上廣泛研究已超過百年，其理論已豐富且深奧，但在當時沒人認為橢圓曲線有何實質用途；自從 Miller（1985）及 Koblitz（1987）兩位學者分別提出橢圓曲線的應用後，橢圓曲線開始在密碼學領域受到重視。與基於大質數因數分解的 RSA 等加密方法不同，其定義為在射影平面上滿足 Weieerstrass 方程式所有點的集

合。在密碼學應用上，則主要應用在有限域 $GF(q)$ 中取質數 p（p>3）同餘的橢圓曲線群，以$E: y^2 = x^3 + ax + b \ (mod \ p)$來表示，其中 a、b 為小於 p 之正整數，且$4a^3 + 27b^2 \neq 0 \ (mod \ p)$。另在橢圓曲線的定義中存在一個元素 O，稱為無窮遠點，一般可視為在 Y 軸上方無窮遠處（張鈞富，2014）；而相比 RSA 等非對稱式加密，其優勢在於安全性相同的前提下，可使用較短的私密金鑰，非常適合在資源有限環境下使用（如智慧卡、智慧型手機及無線行動裝置）。一般認爲，q 位元域上的 ECC，當q的長度爲 160 位元時，其安全性相當於 RSA 演算法使用 1024 位元模數（如表 1）。私密金鑰較短意味著所需要電腦網路的頻寬和記憶體較小，在執行速度方面較現存其他相對應的離散對數密碼系統要快，且在簽名和解密方面也比 RSA 快（Materese, 2016）；此外，假設一個橢圓曲線是屬於F_q，而 G 是橢圓曲線 E 上一點，給定一個屬於橢圓曲線上的點 G'，若要找出一整數 k 使得$kG = G'$，因其特殊的點加法運算，破密者除了逐一窮舉所有可能的點之外，別無他法。直至目前為止，除了建置成本龐大的量子電腦外，此問題仍符合實際安全。

表 1　橢圓曲線密碼系統與 RSA 在相同安全度下金鑰長度之比較表

	金鑰長度					
ECC	112	163	224	256	384	512
RSA	512	1024	2048	3072	7680	15360
金鑰長度比	1：5	1：6	1：9	1：12	1：20	1：30

資料來源：Materese, 2016

背包密碼系統設計思想是把易解背包問題偽裝成一個看似困難的背包問題，其安全性植基於求子集和問題的困難性，假設手邊有一堆物品，其每件物品重量各異之物品表示為（$v_1, v_2, \dots, v_n$）。並以一個背包能固定裝載物品重量計為V，如果知道每件物品的重量時，是比較容易知道找出其物品的組合來裝滿這背包，但若只知道背包的總重量時，要反推有哪些未知物品在背包內時就很困難，此即為背包難題（Odlyzko, 1990）。

$v = v_1 \mathrm{y}_1 + v_2 y_2 + \cdots + v_n \mathrm{y}_n$，其中$v_n \ (\mathrm{i} = 1,2, \cdots \mathrm{n}) \in \{0,1\}$；

$y_i = 0$表示不在背包內，$y_i = 1$表示在背包內。

物體重量的序列$W =$（$v_1', v_2', \dots, v_n'$），其背包向量$\sum_{i=1}^{n} v_n' = v$。（$v_n' = v_n \mathrm{y}_n$）

這個問題，已被證明是一個 NP-Complete 問題（Michael and David, 1979），因此背包密碼系統不是在多項式時間內可解決之問題。基於背包加密系統其優點為加解密較快，缺點是其系統中超增序列的數值密度太低，造成背包密碼系統被破解（Brickell, 1984）。針對背包密碼系統後續有許多學者提出優化，為改良型隨機背包密碼系統（王青龍與趙祥模，2015），提出運用加法及模運算優化其計算時間，另將超遞增背包隱藏在隨機選擇的背包向量中，能抵抗低密度攻擊，其流程如下：

密鑰生成階段：

- 隨機選取任一超遞背包向量$\hat{g} =$（$g_1, g_2, \dots, \mathrm{g}_n$）。
- 任意選取兩個背包量 $\hat{u} =$（$u_1, u_2, \dots, u_n$），$\hat{\mathrm{z}} =$（$z_1, z_2, \dots, z_n$），u_n，z_n均為正整數且滿足$g_n = u_n + z_n$，$n = 1, \dots, n$。
- 隨機取兩個整數F_1和F_2為私鑰，$F_1 \geq \sum_{i=1}^{n} u_n$,$F_2 \geq \sum_{i=1}^{n} z_n$；$gcd$（$F_1, F_2$）=1
- 求出公鑰 A 使用中國餘式定理
- $a = (a_1, a_2, \dots, a_n)$

- $a_n \equiv u_n(\ mod\ F_1), a_n \equiv z_n(\ mod\ F_2\ ), n = 1,2,\ldots,n$

加密階段：

- 將訊息m轉換為二進位 n bit，$(m)_2 \in \{0,1\}$。
- 將訊息$(m)_2$與公鑰A做加密。
- 密文$C = A \times (m)_2$。

解密階段：

- 接收到密文C後，計算訊息m
- $c_p = C\ mod\ F_1$
- $c_q = C\ mod\ F_2$
- 令$g = c_p + c_q$，由g和超遞背包（$g_1, g_2, \ldots, g_n$）便可恢復明文。

三、本研究設計

本研究提出一個有別於傳統的存取控制須依賴龐大資料庫及承受管理負擔與風險等問題之機制設計。此機制角色區分軍種使用者、各軍智慧卡管理系統、國軍雲端服務平臺及國軍認證中心，利用國軍雲端服務平台的分散式架構，整合現有國軍系統，避免各系統僅存放集中式資料庫，並利用智慧卡管理系統整合各系統的金鑰管理，實現一人一卡登入多系統且不同系統擁有不同的存取權限；研究流程則區分為系統初始、註冊申請、驗證取得及服務使用等 4 階段（如圖 3）。

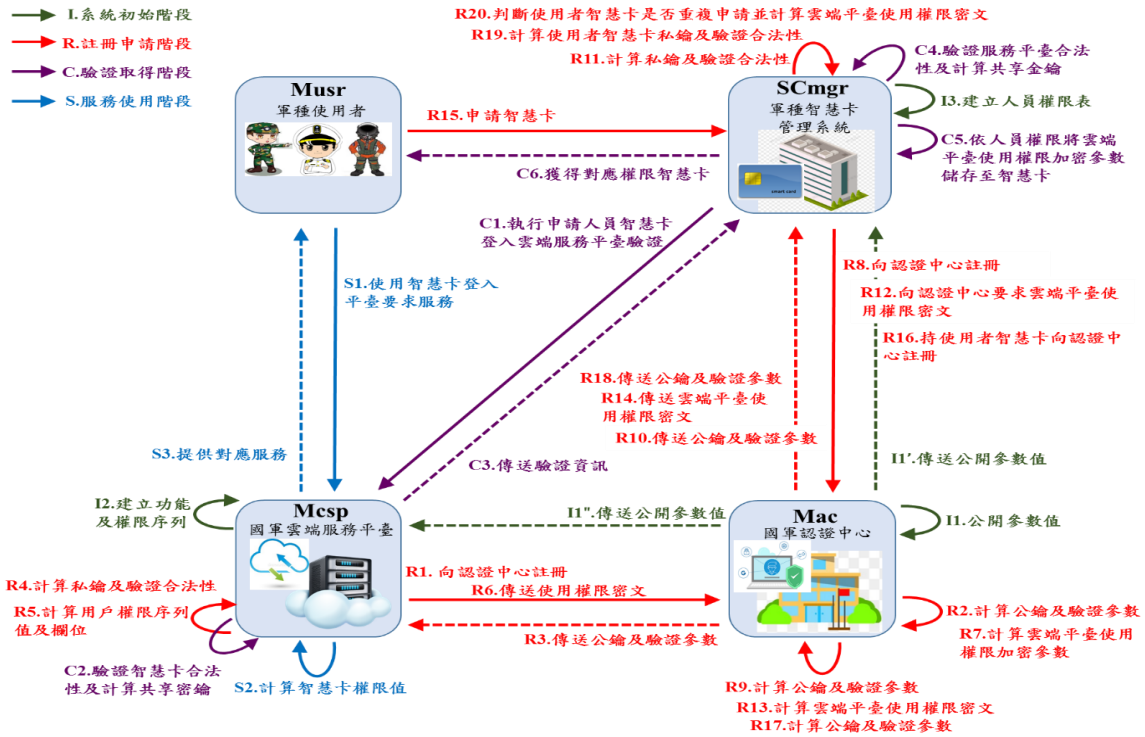

圖 3　研究機制流程圖

3.1 研究參數及符號說明

本研究各階段使用之符號參數，如表 2 所示。

表 2　研究機制符號說明表

項次	符號	說明	項次	符號	說明
1	Musr	軍種使用者	22	rm_x	註冊者 x 選取的隨機參數
2	SCmgr	軍種智慧卡管理系統	23	ID_x	註冊者 x 的身分憑證
3	Mac	國軍認證中心	24	sig_x	註冊者 x 的數位簽章
4	Mcsp	國軍雲端服務平臺	25	SK_{yz}	兩角色 y、z 間的共享金鑰
5	m_{crd}	Musr的國軍智慧卡	26	$AC1_{mgr}$, $AC2_{usr}$	功能使用權限密文
6	$E(F_q)$	橢圓曲線，F_q 為有限域，q為一大於2^{224}以上之大質數	27	AU_{usr}, AT_{usr}	用於計算$AC2_{usr}$權限密文過程參數點
7	n	橢圓曲線上基點的階數（order）	28	rc_{crd}, rc_{csp}	隨機亂數用以建立通訊金鑰
8	G	橢圓曲線中階數為n之基點	29	CK_{us}	Mcsp、m_{crd}的通訊金鑰
9	$\mathcal{O}$	橢圓曲線的無窮遠點	30	(ms_x, ms_y)	Mcsp的公鑰
10	$h()$	單向無碰撞之值雜湊函數	31	(sc_x, sc_y)	SCmgr的公鑰
11	$H()$, $Ver()$	單向無碰撞之點雜湊函數	32	(cr_x, cr_y)	m_{crd}的公鑰
12	u, v / $\bar{u}, \bar{v}$	隨機向量／向量參數（隨機背包）	33	$Ekey_{csp}$	雲端服務平臺對應欄位加密金鑰
13	j_m, k_m, j_n, k_n	隨機參數（隨機背包）	34	$\vec{A}$	Musr所持m_{crd}的加密權限
14	$\tilde{u}$、$\tilde{v}$	超增序列值	35	$\vec{R}$	Mcsp計算出m_{crd}的權限參數點
15	$\hat{u}_{mgr}$、$\hat{v}_{mgr}$	雲端服務平臺使用權限對應表	36	T_{crd}, T_{csp}	m_{crd}、Mcsp的時戳驗證參數
16	uSC_{crd}、vSC_{crd}	使用權限種類值、功能權限值	37	$\underline{T}$	時戳門檻
17	sn_{crd} ad_{crd}	Musr的智慧卡m_{crd}使用（功能）權限對應值	38	$Ver(MspA)$, $Ver(MspB)$	驗證Mcsp身分之參數
18	SK, MK, DK, CK	SCmgr、Mcsp、m_{crd}、Mac公開金鑰	39	$Ver(m_{crd}1)$, $Ver(m_{crd}2)$	驗證m_{crd}身分之參數
19	sk, mk, dk, ck	SCmgr、Mcsp、m_{crd}、Mac私密金鑰	40	RequsetService	Musr向Mcsp請求使用雲端平臺服務
20	id_{mgr}, id_{csp}	SCmgr、Mcsp之身分ID識別	41	AcceptService	Mcsp向Musr回傳是否同意服務訊息
21	rd_x	Mac對應註冊者x選取的隨機參數			

3.2 研究機制各階段流程及演算法

本節分別針對機制設計系統初始、註冊申請、驗證取得及服務使用階段之傳輸內容及步驟做說明。

3.2.1 初始階段

國軍認證中心、軍種智慧卡管理系統及國軍雲端服務平臺在此階段執行後續流程所需參數及權限規劃，作業分述如下：

I1. 國軍認證中心在有限域F_q上，選取一安全橢圓曲線$E\ (F_q)$，並在$E\ (F_q)$上選取一階數為n的基點G，使得 $n \cdot G = O$；接著選定私密金鑰ck後，計算出公開金鑰CK並公開系統相關參數$E\ (F_q)$、G、n、h（）、H（）、Ver（）及CK

$$CK = \ ck \cdot G \tag{1}$$

I2. 國軍雲端服務平臺在此階段建立功能服務及權限對應序列表。

I3. 軍種智慧卡管理系統在此階段建立人員權限表，以利後續人員申請，可依該申請人員權限核發權限對應之國軍智慧卡（m_{crd}）。

3.2.2 註冊申請階段

R1. 國軍雲端服務平臺首先使用國軍認證中心的公開參數，並產生一組隨機參數$rm_{csp} \in [2, n-2]$後，國軍雲端服務平臺將身分識別id_{csp}與國軍認證中心公開參數計算得身分憑證ID_{csp}，將id_{csp}、ID_{csp}傳送至國軍認證中心申請註冊。

$$ID_{csp} = h\left(rm_{csp} \parallel id_{csp}\right) \cdot G \tag{2}$$

R2. 當國軍認證中心收到id_{csp}、ID_{csp}後，選取隨機參數$rd_{csp} \in [2, n-2]$計算出國軍雲端服務平臺的公開金鑰MK及簽章sig_{csp}。

$$MK = \ ID_{csp} + \left(rd_{csp} - h\left(id_{csp}\right)\right) \cdot G = \left(ms_x, ms_y\right) \tag{3}$$

$$sig_{csp} = rd_{csp} + ck\left(ms_x + h\left(id_{csp}\right)\right) \tag{4}$$

R3. 國軍認證中心回傳公開金鑰MK及簽章sig_{csp}給國軍雲端服務平臺。

R4. 國軍雲端服務平臺於接收到公鑰MK、簽章sig_{csp}後，產生自己的私鑰mk，並透過sig_{csp}驗證MK的合法性如下，若驗證符合將建立共享金鑰SK_{cspMac}。

$$mk = sig_{csp} + h\left(rm_{csp} \parallel id_{csp}\right) \tag{5}$$

$$MK' = mk \cdot G \stackrel{?}{=} MK \tag{6}$$

$$SK_{cspMac} = mk \cdot CK = ck \cdot MK \tag{7}$$

R5. 國軍雲端服務平臺分別計算使用者用戶類別與雲端平臺功能服務權限服務向量，並計算使用權限表密文，步驟如下：

- 選擇使用者類別與服務向量，並取隨機四個質數j_m、k_m、j_n與k_n。

取隨機m向量$u = \{u_1, u_2, \ldots, u_m\}$，$u_i$為正整數。 (8)

取隨機n向量$v = \{v_1, v_2, \ldots, v_n\}$，$v_i$為正整數。 (9)

計算向量$\bar{u} = \{\overline{u_1}, \ldots, \overline{u_m}\}$，$\overline{u_i} = u_i - 2^{m-1}$，$i = 1, \ldots, \mathrm{m}$ (10)

計算向量$\bar{v} = \{\overline{v_1}, \overline{v_2}, \ldots, \overline{v_n}\}$，$\overline{v_i} = v_i - 2^{n-1}$，$i = 1, \ldots, n$ (11)

$$j_m > \sum_{i=1}^{m} u_i\text{，}k_m > 2\ max\left\{\sum_{\overline{u_i}>0} \overline{u_i}, -\sum_{\overline{u_i}>0} \overline{u_i}\right\} \tag{12}$$

$$j_n > \sum_{i=1}^{n} v_i\text{，}k_n > 2\ max\left\{\sum_{\overline{v_i}>0} \overline{v_i}, -\sum_{\overline{v_i}>0} \overline{v_i}\right\} \tag{13}$$

- 透過隨選j_m、k_m、j_n與k_n參數，並使用中國餘式定理求出使用者類別與功能服務權限序列值$\tilde{u}$與$\tilde{v}$。

$$\widetilde{u_i} \equiv u_i \ (mod j_m)\ , \widetilde{u_i} \equiv \overline{u_i}\ (mod k_m)\ , i = 1, \dots, m \quad (14)$$

$$\widetilde{v_i} \equiv v_i \ (mod j_n)\ , \widetilde{v_i} \equiv \overline{v_i}\ (mod k_n)\ , i = 1, \dots, n \quad (15)$$

$$\tilde{u} = \{\widetilde{u_1}, \widetilde{u_2}, \dots, \widetilde{u_m}\}，其中\ 0 \le \widetilde{u_i} \le j_m k_m - 1 \quad (16)$$

$$\tilde{v} = \{\widetilde{v_1}, \widetilde{v_2}, \dots, \widetilde{v_n}\}，其中\ 0 \le \widetilde{v_i} \le j_n k_n - 1 \quad (17)$$

- 依軍種使用者軍種使用者使用權限劃分來設定平臺用戶參數$\hat{u}_{mgr}$及功能使用參數$\hat{v}_{mgr}$，並計算出提供軍種使用者使用之國軍智慧卡m_{crd}的使用權限種類值uSC_{crd}、功能權限值vSC_{crd}、使用權限對應值sn_{crd}及功能權限對應值ad_{crd}，再運用與國軍認證中心的共享金鑰SK_{cspMac}計算出權限密文$AC1_{mgr}$。

$$\hat{u}_{mgr} = (\hat{u}_1, \hat{u}_2, \dots, \hat{u}_m), \hat{u}_m \in [0,1] \quad (18)$$

$$\hat{v}_{mgr} = (\hat{v}_1, \hat{v}_2, \dots, \hat{v}_n), \hat{v}_n \in [0,1] \quad (19)$$

$$uSC_{crd} = \sum_{i=1}^{m} \tilde{u} \times \hat{u}_{mgr} \quad (20)$$

$$vSC_{crd} = \sum_{i=1}^{n} \tilde{v} \times \hat{v}_{mgr} \quad (21)$$

$$sn_{crd} = uSC_{crd} \oplus m_{crd} \quad (22)$$

$$ad_{crd} = vSC_{crd} \oplus m_{crd} \quad (23)$$

$$AC1_{mgr} = (uSC_{crd}, sn_{crd} + ad_{crd}) + SK_{cspMac} \quad (24)$$

R6. 國軍雲端服務平臺將權限序列值$\tilde{u}$與$\tilde{v}$權限密文$AC1_{mgr}$傳送至國軍認證中心。

R7. 國軍認證中心使用與國軍雲端服務平臺之共享金鑰SK_{cspMac}，自$AC1_{mgr}$解出uSC_{crd}、vSC_{crd}、sn_{crd}及ad_{crd}，並予以保留，以利後續軍種智慧卡管理系統向國軍認證中心註冊完成後取得。

$$AC1_{mgr} - SK_{cspMac} = (uSC_{crd}, sn_{crd} + ad_{crd}) \quad (25)$$

R8. 軍種智慧卡管理系統首先產生一組隨機參數$rm_{mgr} \in [2, n-2]$後，將身分識別id_{mgr}與國軍認證中心所提供之公開參數執行計算出ID_{mgr}，透過安全通道將id_{mgr}、ID_{mgr}傳送至國軍認證中心提出註冊需求。

$$ID_{mgr} = h\ (rm_{mgr} \| id_{mgr})\ \cdot G \quad (26)$$

R9. 當國軍認證中心接收到id_{mgr}、ID_{mgr}後，選取隨機參數rd_{mgr}計算出軍種智慧卡管理系統的公開金鑰SK及簽章sig_{mgr}。

$$SK = ID_{mgr} + \left(rd_{mgr} - h(id_{mgr})\right) \cdot G = (sc_x, sc_y) \quad (27)$$

$$sig_{mgr} = rd_{mgr} + ck\left(sc_x + h(id_{mgr})\right) \quad (28)$$

R10. 國軍認證中心回傳公開金鑰SK及簽章sig_{mgr}給軍種智慧卡管理系統。

R11. 軍種智慧卡管理系統於接收公開金鑰SK、簽章sig_{mgr}，產生自己的私鑰sk，並透過sig_{mgr}驗證SK的合法性，若驗證符合將建立共享金鑰SK_{mgrMac}。

$$sk = sig_{mgr} + h(rm_{mgr} \| id_{mgr}) \quad (29)$$

$$SK' = sk \cdot G \stackrel{?}{=} SK \quad (30)$$

$$SK_{mgrMac} = sk \cdot CK = ck \cdot SK \quad (31)$$

R12. 軍種智慧卡管理系統向國軍認證中心要求國軍雲端服務平臺的權限序列值$\tilde{u}$與$\tilde{v}$及權限密文$AC1_{mgr}$。

R13. 國軍認證中心使用與軍種智慧卡管理系統之共享金鑰SK_{mgrMac}將國軍雲端服務平臺功能使用權限密文$AC1_{mgr}$進行加密。

$$AC1_{mgr} = (uSC_{crd}, sn_{crd} + ad_{crd}) + SK_{mgrMac} \quad (32)$$

R14. 國軍認證中心向軍種智慧卡管理系統傳送權限序列值$\tilde{u}$與$\tilde{v}$及功能使用權限密文$AC1_{mgr}$，以利後續提供軍種使用者申請國軍智慧卡m_{crd}之用。

R15. 軍種使用者向軍種智慧卡管理系統提出國軍智慧卡m_{crd}申請需求。

R16. 軍種使用者在使用m_{crd}向國軍雲端服務平臺要求功能服務前，須由軍種智慧卡管理系統使用當前申請的m_{crd}與國軍認證中心進行註冊，首先於軍種智慧卡管理系統插入智慧卡m_{crd}及提供一組隨機碼$rm_{crd} \in [2, n-2]$，計算出ID_{crd}後，將ID_{crd}及m_{crd}傳給國軍認證中心提出註冊需求。

$$ID_{crd} = h(m_{crd} \| rm_{crd}) \cdot G \quad (33)$$

R17. 當國軍認證中心接收到ID_{crd}、m_{crd}，選取隨機參數rd_{crd}計算出當前申請M_{crd}的公開金鑰DK及簽章sig_{crd} 。

$$DK = ID_{crd} + \left(rd_{crd} - h(m_{crd})\right) \cdot G = \left(cr_x, cr_y\right) \quad (34)$$

$$sig_{crd} = rd_{crd} + ck\left(cr_x + h(m_{crd})\right) \quad (35)$$

R18. 國軍認證中心回傳當前申請m_{crd}的公開金鑰DK及簽章sig_{crd}給軍種智慧卡管理系統。

R19. 軍種智慧卡管理系統於接收到當前申請m_{crd}的公開金鑰DK、簽章sig_{crd}，產生當前申請m_{crd}的私鑰dk，並透過sig_{crd}驗證DK的合法性，若驗證符合將建立共享金鑰SK_{crdMac} 。

$$dk = sig_{crd} + h(m_{crd} \| rm_{crd}) \quad (36)$$

$$DK' = dk \cdot G \stackrel{?}{=} DK \quad (37)$$

$$SK_{crdMac} = dk \cdot CK = ck \cdot DK \quad (38)$$

R20. 軍種智慧卡管理系統計算國軍雲端服務平臺權限密文，以利後續依申請人員權限給予相關對應使用之權限密文，並判斷當前設定之m_{crd}是否重複申請，程序如下：

- 軍種智慧卡管理系統使用與國軍認證中心之共享金鑰SK_{mgrMac}計算出國軍雲端服務平臺功能使用權限密文$AC1_{mgr}$取得m_{crd}的註冊欄位uSC_{crd}、位置欄位vSC_{crd}、註冊序列值sn_{crd}及位置值ad_{crd}。

$$AC1_{mgr} - SK_{mgrMac} = (uSC_{crd}, sn_{crd} + ad_{crd}) \quad (39)$$

- 透過m_{crd}註冊欄位uSC_{crd}值對應出$\tilde{u}$用戶註冊欄位，並使用註冊參數判斷該m_{crd}是否註冊，若未註冊則建立其欄位加密金鑰$Ekey_{csp}$。

$$AU_{usr} = (x_1, x_2) = \left((uSC_{crd}, sn_{crd} + ad_{crd}) + Ekey_{csp}\right) \quad (40)$$

- 軍種智慧卡管理系統依當前軍種使用者權限等級所持之m_{crd}對應功能使用權限計算出加密之權限表$AC2_{usr}$。

$$AC2_{usr1} = rd_{mgr} \cdot \mathrm{G} \quad (41)$$

$$AT_{usr} = rd_{mgr} \cdot SK = (y_1, y_2) \quad (42)$$

$$AC2_{usr2} = AU_{usr} \cdot AT_{usr} = (x_1 \cdot y_1, x_2 \cdot y_2) = (z_1, z_2) \quad (43)$$

$$AC2_{usr} = \{AC2_{usr1}, AC2_{usr2}\} \quad (44)$$

3.2.3 驗證取得階段

軍種智慧卡管理系統使用當前軍種使用者申請之m_{crd}協助完成第一次連線認證作業，當作業完成後，由軍種智慧卡管理系統依當前軍種使用者權限提供對應m_{crd}，軍種使用者下次登入時可直接使用國軍雲端服務平臺之功能，程序為 C1 至 C6。

C1. 軍種智慧卡管理系統使用m_{crd}初次連線登入至國軍雲端服務平臺時，m_{crd}會先傳送時戳參數T_{crd}與國軍雲端服務平臺的時戳參數T_{csp}進行驗證，通過後即提供連線，若未能通過則中斷聯線，成功連線後則進行雙方身分驗證，並計算出共享金鑰及 Diffie-Hellman 金鑰傳送至國軍雲端服務平臺，程序如下：

- m_{crd}與國軍雲端服務平臺初次連線執行時戳參數驗證計算是否符合時戳門檻$\underline{T}$。

$$\left(T_{crd} - T_{csp}\right) \leq \underline{T} \quad (45)$$

- m_{crd}與國軍雲端服務平臺驗證符合時戳門檻$\underline{T}$連線後，互相驗證身分是否合法。

$$dk' = DK + \ h(m_{crd}) \cdot G + \left(cr_x + h(m_{crd})\right) \cdot CK \quad (46)$$

$$dk \stackrel{?}{=} dk' \quad (47)$$

$$mk' = MK + h\left(id_{csp}\right) \cdot G + \left(ms_x + h\left(id_{csp}\right)\right) \cdot CK \quad (48)$$

$$mk \stackrel{?}{=} mk' \quad (49)$$

- m_{crd}建立隨機參數rc_{crd}後利用所選之橢圓曲線G點計算出驗證點參數RC_{crd}，並計算出共享金鑰SK_{cspcrd}及 Diffie-Hellman金鑰$DHRC_{crd}$後傳至國軍雲端服務平臺。

$$RC_{crd} = rc_{crd} \cdot G \quad (50)$$

$$SK_{cspcrd} = mk \cdot DK = dk \cdot MK \quad (51)$$

$$DHRC_{crd} = RC_{crd} + SK_{cspcrd} \quad (52)$$

C2. 國軍雲端服務平臺建立隨機參數rc_{csp}後利用所選之橢圓曲線G點計算出驗證點參數RC_{csp}，並計算出共享金鑰SK_{cspcrd}及雙方 Diffie-Hellman 金鑰DH_{us}後，求出雙方通訊金鑰CK_{us}。

$$RC_{csp} = rc_{csp} \cdot G \quad (53)$$

$$SK_{cspcrd} = dk \cdot MK = mk \cdot DK \quad (54)$$

$$DHRC_{csp} = RC_{csp} + SK_{cspcrd} \quad (55)$$

$$RC_{crd} = DHRC_{crd} - SK_{cspcrd} \quad (56)$$

$$DH_{us} = rc_{csp} \cdot RC_{crd} \quad (57)$$

$$CK_{us} = DH_{us} + SK_{cspcrd} \quad (58)$$

C3. 國軍雲端服務平臺傳送驗證參數至m_{crd}。

$$Ver(McspA) = H\left(m_{crd} \parallel id_{csp} \parallel DH_{us}\right) \quad (59)$$

$$Ver(McspB) = H\left(m_{crd} \parallel id_{csp} \parallel CK_{us}\right) \quad (60)$$

C4. m_{crd}驗證參數及比對確認合法性，並回傳$Ver(m_{crd}2)$參數至國軍雲端服務平臺驗證是否正確。

$$RC_{csp} = DHRC_{csp} - SK_{cspcrd} \quad (61)$$

$$DH_{us}{}' = rc_{crd} \cdot RC_{csp} \quad (62)$$

$$CK_{us}{}' = DH_{us}{}' + SK_{cspcrd} \quad (63)$$

$$Ver(m_{crd}1) = Ver(McspA) \quad (64)$$

$$Ver(m_{crd}2) = H\left(m_{crd} \parallel id_{csp} \parallel CK_{us}{}'\right) \quad (65)$$

C5. 軍種智慧卡管理系統運用國軍雲端服務平臺、m_{crd}的通訊金鑰CK_{us}計算出智慧卡加密權限$\vec{\mathrm{A}}$並依人員權限等級將對應權限儲存至m_{crd}中。

$$\vec{\mathrm{A}} = AC2_{usr} + CK_{us} \quad (66)$$

軍種使用者取得對應職務權限之國軍智慧卡m_{crd}。

3.2.4 服務使用階段

在軍種使用者使用國軍雲端服務平臺服務前，須用智慧卡m_{crd}與國軍雲端服務平臺完成持有權限運算後，始可使用其提供之服務及功能。

S1. 軍種使用者運用儲存於智慧卡m_{crd}內之通訊金鑰CK_{us}解出加密之權限表$AC2_{mgr}$後，向國軍雲端服務平臺傳送請求使用雲端平臺服務 RequsetService 訊息及服務權限加密參數$AC2_{usr}$。

$$AC2_{usr} = \vec{\mathrm{A}} - CK_{us} \quad (67)$$

S2. 國軍雲端服務平臺在接收請求功能使用申請 RequsetService 及服務權限加密參數$AC2_{usr}$後，執行當前軍種使用者所持之m_{crd}服務權限計算出$\vec{\mathrm{R}}$，並自$AC2_{usr}$解出雲端服務平臺用戶及位址加密欄位，再依m_{crd}註冊欄位金鑰後解出軍種使用者可使用的功能。

$$\vec{\mathrm{R}} = (r_1, r_2) = mk \cdot AC2_{usr1} = rd_{csp} \cdot (G \cdot mk) = rd_{csp} \cdot MK \quad (68)$$

$$AU_{usr} = \left(AC2_{usr2} \cdot \vec{\mathrm{R}}^{-1} \right) = (x_1, x_2) \quad (69)$$

$$(uSC_{crd}, sn_{crd} + ad_{crd}) = AU_{usr} - Ekey_{csp} \quad (70)$$

$$ad_{crd} = (sn_{crd} + ad_{crd}) - \left(uSC_{crd} \oplus m_{crd} \right) \quad (71)$$

$$vSC_{crd} = ad_{crd} \oplus m_{crd} = (vSC_{crd} \oplus m_{crd}) \oplus m_{crd} \quad (72)$$

$$\left(\hat{u}_{mgr} \right)_2 = (uSC_{crd} modj_m) - \left(uSC_{crd} modk_m \right) \quad (73)$$

$$\left(\hat{v}_{mgr} \right)_2 = (vSC_{crd} modj_n) - \left(vSC_{crd} modk_n \right) \quad (74)$$

S3. 國軍雲端服務平臺運用彼此通訊密鑰CK_{us}將當前軍種使用者所持之m_{crd}服務權限加密後回傳 AcceptService 訊息供軍種使用者正常使用服務。

四、安全性與效益分析

現行國軍跨軍種資料交換基於資安考量，且無身分辨證機制，故無建立軍種間雲端資料交換空間，仍以實體及檔案加密後以信箱或點對點方式傳輸給對方執行；而各類雲端系統，係各軍種使用者輸入 AD 帳號及密碼做為系統登入方式，若無有效及更安全的身分驗證機制，將導致不法人士偽冒侵入攻擊情事發生，並可能產生使用者帳戶遭不法人士盜取，延伸出機敏資料或情資外洩。本章節主要針對經研究後所提之強化及改善機制的安全性分析進行探討並與現有機制進行比較。

4.1 機密性

本研究機制註冊申請階段中，Mcsp可就Musr層級類別中配賦雲端服務平臺使用權限表，將Musr相關註冊資訊送至Mac；透過Mac計算Musr之使用權限表密文$AC1_{mgr}$（如圖 3 R13）及Musr並透過智慧卡m_{crd}安全存放$\overline{A}$訊息（如圖 3 C5）達到多因子認證方式。

倘若不法人士想偽冒使用者身分，除了須擁有智慧卡多因子認證外，欲使用中間人攻擊方式來取得解密密文時，首先要破解並取得雲端服務平臺Mcsp提供m_{crd}註冊、位置欄位與序列值加密金鑰（如圖 3 S1-2）而將面對橢圓曲線離散對數難題；即使不法人士以其他不當的方式取得欄位及權限類別序列值後，也須要解出欄位及權限類別序列，屆時將面臨隨機背包難題而無法輕易破解。

4.2 完整性

本研究機制註冊申請階段中，Mcsp、SCmgr及使用者m_{crd}選取隨機參數，計算各自身分憑證（如圖 3 R1-2、R8-9 及 R16-17）後傳送至Mac；經Mac雜湊運算並結合SCmgr、Mcsp及使用者m_{crd}之身分憑證後，分別產生數位簽章並相互完成認證。

不法人士若欲破解將面臨單向雜湊函數及橢圓曲線離散難題；就算取得認證中心管理權限存取資料，但未能獲得私鑰（如圖 3 I1），或是竊得共享金鑰，否則將面對橢圓曲線解離散對數難題。

4.3 可用性

本研究機制驗證取得階段中，SCmgr協助Musr申請之m_{crd}與Mcsp確認彼此身分無誤後，m_{crd}與Mcsp將相互執行交換共享金鑰（如圖 3 C1）與通訊之金鑰（如圖 3 C2）；而在服務使用階段Musr所持之m_{crd}使用Mcsp服務時，Mcsp再依據Musr所持之m_{crd}之對應權限（如圖 3 S2），將彼此間的通訊金鑰運算出結果後以加密後回傳AcceptService訊息至Musr所持之m_{crd}來同意使用雲端服務平臺之各項功能與服務。

不法人士欲偽冒Musr或Mcsp身分時，須面臨橢圓曲線離散對數難題，使不法人士因無授權沒辦法通過身分驗證而終止連線服務，亦可避免Mcsp遭重送式攻擊（Replay attack）而造成的服務中斷，避免Musr因無法執行對應服務而影響業務執行成效。

4.4 不可否認性

本研究機制驗證取得階段中，SCmgr使用當前Musr申請之m_{crd}將產生雲端服務平臺欄位權限密文，而Musr申請之m_{crd}與Mcsp間生成共享金鑰（如圖 3 C1）與通訊金鑰（如圖 3 C2）；在後續於服務使用階段中，Musr所持之m_{crd}提出資料存取及功能服務時，Mcsp再依據Musr所持之m_{crd}身分別及功能使用權限，運算結果以其通訊金鑰加密後，回傳Musr

在本研究機制服務使用階段中，Mcsp以其私鑰解密且產製通訊金鑰（如圖 3 C2）過程中，其Musr所持之m_{crd}與Mcsp之個人資訊亦包含其中（如圖 3 C4 及 S2），彼此無法否認雙方之前所執行過的關鍵行為。

4.5 存取控制

本研究機制驗證取得階段中，首先將驗證當前申請之m_{crd}與Mcsp雙方時戳（如圖 3

C1），保證在時效內連線，否則將取消，通過後將依照Musr所持之m_{crd}應俱備之權限等級，以序列方式定義權限表並利用隨機背包密碼系統計算Mcsp於註冊申請階段向Mac註冊之功能權限值及權限表（如圖 3 R5）；於服務使用階段中，僅回傳當前申請之m_{crd}雲端服務平臺使用權限之運算結果。

若發生未授權人士盜用Musr身分，利用Musr來向Mcsp提出雲端服務平臺使用服務時，將經過Mcsp驗證，期間Mcsp判斷為非法授權用戶，Mcsp將否絕其服務使用之請求，以達存取控制與使用權管控之目的；而在使用者Musr所持之m_{crd}遭人盜用情況下，也因無法得知該Musr所設定之m_{crd}個人密碼導致無法使用。

4.6 身分認證

本研究機制註冊申請階段中， Mcsp及Musr申請之m_{crd}向Mac完成註冊後獲得各自公鑰及簽章後（如圖 3 R2-4 及 R17-19），相互傳送認證資訊而無須與Mac保持連線，可離線相互完成身分認證後，建立共享金鑰與通訊金鑰，以Musr申請之m_{crd}對Mcsp實施認證為例（如圖 3 C1）。

Musr及Mcsp雙方執行身分認證時，在持有對方之公開認證資訊與Mac之公鑰，可不用經過Mac來獨立進行身分認證。若不法人士欲偽裝Musr或Mcsp身分時，將面臨橢圓曲線離散對數難題而被否決；另外再驗證取得階段中，智慧卡管理系統SCmgr以標準政策給予合法使用者所能擁有之權限，防止未經授權使用者構連藉以提升系統安全性。

4.7 抗同謀碰撞攻擊

本研究機制註冊申請階段中，Musr申請之m_{crd}公鑰及私鑰非直接由Mac產製及保管，為結合身分識別、簽章、隨機參數（如圖 3 R16-17）及Mac之隨機參數計算出來的，用以避免遭非授權人員與Mac串聯肆意竊取。

本研究機制中，Mac僅參與計算公鑰過程，無法直接產生、偽造Musr申請之m_{crd}私鑰，且Mac未參與服務使用階段，故Mcsp以私鑰並非透過Mac解密資訊取得Musr所持之m_{crd}相關權限值資料，有效避免非授權人員藉Mac擁有多項參數之便，防阻同謀攻擊。

4.8 資料保密

本研究機制註冊申請階段中，由Mcsp產生超增序列值（如圖 3 R5）提供Musr使用m_{crd}對應的註冊欄位、位置欄位、註冊序列值及位置值建立加密參數。

若不法人士欲由數值反推註冊欄位定義及權限序列，將面臨破解隨機背包難題，而欲破解權限值密文時，亦將面臨破解橢圓曲線離散對數難題而難以達成。

4.9 本研究與現行機制安全性分析比較

表 3 係針對現有雲端系統運作機制與本研究設計之基於橢圓曲線密碼系統並導入多因子身分認證協定機制進行各項安全比較，可發現本機制除符合機密性、存取控制之要求外，亦就可用性及連線資料保密進行改良精進與補足完整性、不可否認性、身分認證及抗同謀攻擊之不足處，故本研究可達到安全性要求；為配合雲端高速運算模型，近年發表雲端服務存取權限機制研究皆是以雙線性曲線對（bilinear pairing）進行加密（Wu

et al., 2017; Deng et al., 2020），雙線性曲線對起初應用於密碼學是為了將 ECDLP 問題歸約到 DLP 問題而被提出（Menezes et al., 1993），因此在相同長度的金鑰下，破譯雙線性曲線對的時間將大幅縮短；為了解決上述問題許多學者提出相應的方案，其中以 Boneh（2001）等人提出的 BLS 簽章演算法最為著名，該演算法可以有效縮減簽章的位元組大小，但是將簽章複雜度提升，驗證時間相對于傳統的 ECDSA 簽名則因此上升了兩個單位量級；考量現行系統運作機制，在資料儲存空間上非常充足，且為了在一定的安全性上保有較佳的驗證效能，因此本研究設計之機制較為適合。

4.10 執行效能分析

本節以葉昱宗（2015）所提之參考表為基準（如圖 4），針對本研究所提機制之效益評估整理各階段運算成本概估，且考量本研究屬國軍客製化系統且原系統無相關參照演算法，故無從比較，僅針對本研究設計機制執行各事件之運算成本（如圖 5）

表 3　本研究與現行系統之安全比較表

項次	比較項目	現行系統運作機制		本研究設計之機制	
1	機密性	使用者僅輸入 AD 帳號密碼來登入系統，此登入方式無法驗證是否為合法使用者。	△	使用者均須完成註冊與執行身分認驗證後，並搭配智慧卡多因子認證，才能連線雲端服務平臺要求功能服務（如圖 3 R15-17 及 C4）。	∨
2	完整性	未使用雜湊函數或 RSA 數位簽章等方法，無法確保資訊傳遞間之完整性。	×	不法人士若欲偽冒使用者簽章或竄改，則會面對破解單向無碰撞雜湊函數及橢圓曲線離散對數難題，將無法輕易破解（如圖 3 R19）。	∨
3	可用性	目前僅利用防火牆阻擋可疑來源位址及 AD 帳密列表，但對於未紀錄於防火牆的名單，將會面臨重送式攻擊。	△	使用者若未能與雲端服務平臺完成身分驗證，將限制或拒絕該使用者與雲端服務平臺連線，使雲端服務平臺能抵禦重送式攻擊（如圖 3 S2）。	∨
4	不可否認性	目前使用者僅註冊固定憑證，使用者於執行動作之後，將有可能遭遇到事後否認行為。	×	運用智慧卡及個人帳密等方式，雙方須使用共同通訊金鑰，資訊傳達可避免曾執行過的關鍵事件或動作遭到否認(如圖 3 C2、C4 及 S2)。	∨
5	存取控制	目前運用使用者 AD 帳密列表限制登入，若帳密列表遭盜用將可能面臨各項資料外洩。	△	首先運用時戳來限制服務申請及登入認證，並結合隨機背包密碼系統，給予使用者功能權限，若判斷為非授權時間或身分，將拒絕功能服務使用之申請(如圖 3 R5 及 C1)。	∨
6	身分認證	目前僅使用使用者 AD 帳密列表限制登入，沒有第三方安全認證機制。	△	因應軍種及層級權限特性，為了降低使用者對第三方認證系統之依賴，採用採自我認證機制，以達於受限網路環境下依然能完成相關	∨

				認證連線（如圖 3 C1）。	
7	抗同謀攻擊	管理方式為採主從管控，若管理人員其管理系統身分帳密遭偽冒或盜用，則使用者將失去安全保障。	×	本研究運用離線自我認證方式，在雲端服務平臺計算使用者權限密文及使用者使用服務存取功能時，認證伺服器都未參加，故能抵禦同謀攻擊（如圖 3 C1）。	∨
8	資料保密	僅使用 AD 帳密列表限制登入，但無多因子認證機制，且使用者間傳輸資料僅仰賴使用者檔案資料加密習慣，若遺忘加密密碼或常使用廣泛加密密碼時，將造成洩密及業務延宕情事。	△	本研究將具有橢圓曲線離散對數及隨機背包雙重難題，藉此保護使用者及雲端服務平臺所計算出權限密文，以保障服務及使用者傳輸資料安全（如圖 3 R4、R5 及階段 I）。	∨
附註：∨代表符合、△代表部分符合、x代表不符合					

符號	定義	運算成本
T_{MUL}	執行一次模式乘法運算所需時間	參考備註一
T_{ECMUL}	執行一次 ECC 乘法運算所需時間	$29T_{MUL}$
T_{ECADD}	執行一次 ECC 加法運算所需時間	$5T_{MUL}$
T_{INVS}	執行一次模式乘法反元素運算所需時間	$240T_{MUL}$
T_{EXP}	執行一次模式指數運算所需時間	$240T_{MUL}$
t_h	執行一次值雜湊函數所需時間	$0.4T_{MUL}$
T_h	執行一次點雜湊函數所需時間	$23T_{MUL}$
$T_{\sum mul}$	執行一次數值序列乘法運算所需時間	參考備註二
$T_{\sum add}$	執行一次數值序列加法運算運算所需時間	參考備註三
T_{ADD}	執行一次模式加法運算所需時間	因運算時間短，可忽略不計
$T_{\oplus}$	執行一次 XOR 運算所需時間	
$T_{\|}$	執行一次串接運算所需時間	
備註： 一、本研究僅以T_{MUL}作為運算成本計算基準，詳細視不同機器，規格及執行環境而異。 二、$T_{\sum mul}$:若該序列長度為 n，則成本為nT_{MUL} 三、$T_{\sum add}$若該序列長度為 n，則成本為$(n-1)T_{ADD}$		

圖 4　運算成本參考

（資料來源：葉昱宗，2015）

事件	運算式	運算成本概估
初始階段	$CK = ck \cdot G$	$1T_{ECMUL}$
Subtotal		$29T_{MUL}$
註冊申請階段	$ID_{csv} = h(rm_{csv} \parallel id_{csv}) \cdot G$ $MK = ID_{csv} + (rd_{csp} - h(id_{csv})) \cdot G$ $sig_{csv} = rd_{csv} + ck\,(ms_x + h(id_{csv}))$ $mk = sig_{csv} + h(rm_{csv} \parallel id_{csv})$ $MK' = mk \cdot G = MK$ $SK_{csvMac} = mk \cdot CK = ck \cdot MK$ 上述為Mcsp本階段步驟，SCmgr及m_{crd}註冊步驟同上 $uSC_{crd} = \sum_{i=1}^{m} \tilde{u} \times \hat{u}_{mar}$ $vSC_{crd} = \sum_{i=1}^{n} \tilde{v} \times \hat{v}_{mar}$ $sn_{crd} = uSC_{crd} \oplus m_{crd}$ $ad_{crd} = vSC_{crd} \oplus m_{crd}$ $AC1_{mar} = (uSC_{crd}, sn_{crd} + ad_{crd}) + SK_{csvMac}$ $AC1_{mar} - SK_{csvMac} = (uSC_{crd}, sn_{crd} + ad_{crd})$ $AU_{usr} = (x_1, x_2) = ((uSC_{crd}, sn_{crd} + ad_{crd}) + Ekey_{csv})$ $AC2_{usr1} = rd_{mar} \cdot G$ $AT_{usr} = rd_{mar} \cdot SK = (y_1, y_2)$ $AC2_{usr2} = AU_{usr} \cdot AT_{usr} = (x_1 \cdot y_1, x_2 \cdot y_2) = (z_1, z_2)$	$T_{ECMUL}+1t_h+T_{\parallel}$ $T_{ECMUL}+T_{ECADD} + t_h$ $T_{ECMUL}+T_{ADD} + t_h + T_{MUL}$ $T_{ADD} + t_h+T_{\parallel}$ T_{ECMUL} $2T_{ECMUL}$ 上述成本乘以 3 $nT_{\nabla mul} + (m-1)T_{ADD}$ $mT_{\nabla mul} + (n-1)T_{ADD}$ $T_{\oplus}$ $T_{\oplus}$ T_{ECADD} T_{ECADD} T_{ECADD} T_{ECMUL} T_{ECMUL} T_{ECMUL}
Subtotal		$(639.3+m+n)T_{MUL}+(m-1)T_{ADD} + (n-1)T_{ADD}$
驗證取得階段	$dk' = DK + h(m_{crd}) \cdot G + (cr_x + h(m_{crd})) \cdot CK$ $mk' = MK + h(id_{csv}) \cdot G + (ms_x + h(id_{csv})) \cdot CK$ $RC_{crd} = rc_{crd} \cdot G$ $SK_{csvcrd} = mk \cdot DK = dk \cdot MK$ $DHRC_{crd} = RC_{crd} + SK_{csvcrd}$ $RC_{csv} = rc_{csv} \cdot G$ $SK_{csvcrd} = dk \cdot MK = mk \cdot DK$ $DHRC_{csv} = RC_{csv} + SK_{csvcrd}$ $RC_{crd} = DHRC_{crd} - SK_{csvcrd}$ $DH_{us} = rc_{csv} \cdot RC_{crd}$ $CK_{us} = DH_{us} + SK_{csvcrd}$ $Ver(McspA) = H(m_{crd} \parallel id_{csv} \parallel DH_{us})$ $Ver(McspB) = H(m_{crd} \parallel id_{csv} \parallel CK_{us})$ $RC_{csv}' = DHRC_{csv} - SK_{csvcrd}$ $DH_{us}' = rc_{crd} \cdot RC_{csv}$ $CK_{us}' = DH_{us}' + SK_{csvcrd}$ $Ver(m_{crd}1) = Ver(McspA)$ $Ver(m_{crd}2) = H(m_{crd} \parallel id_{csv} \parallel CK_{us}')$ $\bar{A} = AC2_{usr} + CK_{us}$	$2T_{ECMUL}+2T_{ECADD} + t_h+T_{ADD}$ $2T_{ECMUL}+2T_{ECADD} + t_h+T_{ADD}$ T_{ECMUL} $2T_{ECMUL}$ T_{ECADD} T_{ECMUL} $2T_{ECMUL}$ T_{ECADD} T_{ECADD} T_{ECMUL} T_{ECADD} $T_h + 3T_{\parallel}$ $T_h + 3T_{\parallel}$ T_{ADD} T_{ECMUL} T_{ECADD} $T_h + 3T_{\parallel}$ $T_h + 3T_{\parallel}$ T_{ECADD}
Subtotal		$445.6T_{MUL}$
服務使用階段	$AC2_{usr} = \bar{A} - CK_{us}$ $R = (r_1, r_2) = mk \cdot AC2_{usr1}$ $AU_{usr} = (AC2_{usr2} \cdot \bar{R}^{-1}) = (x_1, x_2)$ $(uSC_{crd}, sn_{crd} + ad_{crd}) = AU_{usr} - Ekey_{csv}$ $vSC_{crd} = ad_{crd} \oplus m_{crd} = (vSC_{crd} \oplus m_{crd}) \oplus m_{crd}$ $(\hat{u}_{mar})_2 = (uSC_{crd} mod j_m) - (uSC_{crd} mod k_m)$ $(\hat{v}_{mar})_2 = (vSC_{crd} mod j_n) - (vSC_{crd} mod k_n)$	T_{ECADD} T_{ECMUL} T_{INVS} T_{ECADD} $T_{\oplus}$ T_{ADD} T_{ADD}
Subtotal		$279T_{MUL}$
Total		$(1392.9+m+n)T_{MUL} + (m-1)T_{ADD} + (n-1)T_{ADD}$
備註：本研究屬客製化系統設計，考量原系統無相關參照演算法，故無從比較。		

圖 5　運算成本

五、結論

本研究機制利用橢圓曲線加密金鑰長度短與隨機背包密碼系統運算效能快的優點，且適用於國軍雲端服務之身分認證暨金鑰交換機制。在系統運作機制方面，現有國軍系統雖有雲端整合的案例，但僅有在資料儲存時避免了單一資料庫儲存，且在使用權限上較難整合，因此在擴展性上有諸多限制；而本研究透過存取控制之設計，可使各部會系統更容易導入，並且讓使用者不必保管過多的金鑰儲存工具，或是需要記住不同系統的帳號密碼；另在安全性方面，本研究設計在小幅度增加加、解密長度及處理時間的前提下，配合多因子認證，使國軍在跨軍種資料交換及使用各項雲端服務時，具備更高的安全性，能防止用戶端偽冒、不法人士攻擊及抵禦竊聽，並且藉由求解隨機背包密碼系統之難題，將雲端服務平臺功能及使用者權限均透過序列方式隱藏，大幅增加惡意人士獲取權限開通內容之難度，最後採離線自我認證之方式，可讓使用者在取得對應之權限智慧卡後，在無須依賴第三方認證中心情況下與雲端服務平臺完成相互認證，有效縮短作業時間，且可保持服務提供大幅增加可用性。

六、國防領域之應用

本研究針對軍種資料交換及國軍雲端服務架構提出透過多因子執行強化自我認證與存取控制，並運用橢圓曲線密碼系統與隨機背包機加密系統可提升安全性與效率。國軍發揮戰力有賴於各軍種間所偵獲敵情之共享，本研究提供建立適當資訊安全防護的參考，除確保我軍資訊傳輸系統具備高安全及高效能，未來亦可針對跨部門資訊系統進行客製化設計與評估運用，達到支援網狀化作戰效益，並藉由建置雲端服務來改善資源佈署、資安防護及任務遂行等，以利在人力精簡狀況下，不影響任務遂行，以建構多層次資安防護安全機制，且符合相關法規安全述求下更有效發揮國防事務之堅強戰力。

參考文獻

王子承（2017），俄國首次承認組建「網軍」歐洲多國擔心大選遭干預，*上報*。取自 https://www.upmedia.mg/news_info.php?SerialNo=12674。

王青龍、趙祥模（2015），隨機背包公鑰密碼的分析與改進，*計算機科學*，42（6），158-161。

中共國防部（2019），《新時代的中國國防》白皮書。取自 http://www.scio.gov.cn/ztk/dtzt/39912/41132/41134/Document/1660318/1660318.htm。

中共新聞網（2018），習近平談網絡安全：沒有網絡安全就沒有國家安全，取自 http://cpc.people.com.cn/xuexi/BIG5/n1/2018/0817/c385476-30234135.html。

張鈞富（2014），*具自我認證之安全並存簽章方法*，國防大學資訊管理學系研究所碩士論文。

黃建衛（2011），網際網路服務使用者身分驗證機制之安全性研析，財金資訊股分有限公司網站。取自 https://www.fisc.com.tw/tc/knowledge/quarterly1.aspx?PKEY=0abc938c-0f9b-4ed3-a131-8c9ff86e946b。

劉嘉偉、張家瑛（2021），面對中共網軍威脅國軍資訊網路安全之探討，*海軍學術雙月刊*，55（3），118-131。

鄧安文（2018），*密碼學－密碼分析與實驗（第三版）*，全華圖書股分有限公司。

Abdulla, N., & Erçelebi, E. (2017). Identify cloud security weakness related to authentication and identity management (IAM) using openstack keystone model. In International Conference on Engineering and Technology, Computer, Basics and Applied Sciences (pp. 1-5).

A. Menezes, T. Okamoto, and S. A. Vanstone, (1993) Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Trans. Inform. Theory*, vol. 39, no. 5, pp. 1,639-1,646.

Boneh, D., Lynn, B., & Shacham, H. (2001, December). Short signatures from the Weil pairing. *In International conference on the theory and application of cryptology and information security* (pp. 514-532). Springer, Berlin, Heidelberg.

Brickell, E.F., (1984), August. Breaking iterated knapsacks. In Workshop on the Theory and Application of Cryptographic Techniques, pp. 342-358.

Brummett, T., Sheinidashtegol, P., Sarkar, D., & Galloway, M. (2015, November). Performance metrics of local cloud computing architectures. In 2015 ieee 2nd international conference on cyber security and cloud computing (pp. 25-30). IEEE.

Cloud Security Alliance - CSA, Top Threats Working Group (2013)., The Notorious Nine - Cloud Computing Top Threats in 2013. http://www.cloudsecurityalliance.org/topthreats.

Cloud Security Alliance - CSA, Top Threats Working Group (2011)., "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0," Cloud Computing Alliance, http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

Deng, H., Qin, Z., Wu, Q., Guan, Z., Deng, R. H., Wang, Y., & Zhou, Y. (2020). Identity-based encryption transformation for flexible sharing of encrypted data in public cloud. IEEE Transactions on Information Forensics and Security, 15, 3,168-3,180.

Eucalyptus Systems. (2012). Inc.: Eucalyptus Identity and Access Management (IAM)2012. Retrieved from https://www.eucalyptus.com/docs/eucalyptus/4.0/security-guide/security_bp_access.html.

Habiba, U., Masood, R., Shibli, M. A., & Niazi, M. A. (2014). Cloud identity management security issues & solutions: a taxonomy. Complex Adaptive Systems Modeling, 2(1), 1-37.

Hewlett Packard Enterprise Development. (2017). HPE Helion Eucalyptus, Remote Unauthorized Access, Unauthorized Modification, Unauthorized Disclosure of Information.

Retrieved from https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c05363782.
Koblitz, N., (1987), Elliptic Curve Cryptosystems, *Mathematics of Computation American Mathematical Society* (48) , 203-209.
Kumar, R., Gupta, N., Charu, S., Jain, K., & Jangir, S. K. (2014). Open source solution for cloud computing platform using OpenStack. International Journal of Computer Science and Mobile Computing, 3(5), 89-98.
Lamport, L. (1981). Password authentication with insecure communication. Communications of the ACM, 24(11), 770-772.
Materese, R., (2016). Recommendation for Key Management, Part 1: General.
Mell, P., & Grance, T. (2011), The NIST definition of cloud computing, National Institute of Standards and Technology Spec. Publ.
Michael, R., and David, S., (1979), Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman & Co., Freeman, New York.
Miller, V. S., (1985), Use of Elliptic Curve in Cryptography, *Advance in Cryptography-Crypto*, New York: Spring-Verlag , 417-426.
Odlyzko, A.M., (1990). The rise and fall of knapsack cryptosystems. Cryptology and computational number theory, 42, 75-88.
Ren, Y., Ding, N., Wang, T., Lu, H., & Gu, D. (2016). New algor ithms for verifiable outsourcing of bilinear pairings. Science China Information Sciences, 59(9), 99103.
Uzunkol, O., Kalkar, Ö., & Sertkaya, I. (2017). Fully Verifiable Secure Delegation of Pairing Computation: Cryptanalysis and An Efficient Construction. IACR Cryptol. ePrint Arch., 2017, 1173.
Wu, L., Zhang, Y., Choo, K. K. R., & He, D. (2017). Efficient and secure identity-based encryption scheme with equality test in cloud computing. Future Generation Computer Systems, 73, 22-31.