【主題類別】雲端計算架構(Cloud Computing Architecture)

雲端環境下資料保護架構之研究
Study of Data Protection Architecture in Cloud Environment

劉江龍	陳緯修	董德國
國防大學理工學院	國防大學理工學院	國防大學理工學院
教授	博士班研究生	副教授

聯絡人：劉江龍
電 話 ：03-3809991 ext.261
傳 真 ：03-3801407
E-mail：chianglung.liu@gmail.com
地 址 ：桃園縣大溪鎮石園路 75 號電機電子系

雲端環境下資料保護架構之研究
Study of Data Protection Architecture in Cloud Environment

劉江龍 教授
國防大學理工學院電機電子系
Chiang-Lung Liu
Department of Electrical and Electronic Engineering,
Chung Cheng Institute of Technology,
National Defense University
Email: chianglung.liu@gmail.com

陳緯修 博士班研究生
國防大學理工學院國防科學研究所
Wei-Hsiu Chen
School of Defense Science,
Chung Cheng Institute of Technology,
National Defense University
Email: dtchentw@gmail.com

董德國 副教授
國防大學理工學院電機電子系
Der-Kuo Tung
Department of Electrical and Electronic Engineering,
Chung Cheng Institute of Technology,
National Defense University
Email: derektdk@gmail.com

摘 要

雲端運算所帶來的高效能運算及高儲存容量，讓使用者享受到存取便利且成本低廉的各式服務，雲端運算已經成為目前各大企業競相發展的一種創新服務模式；然而，隨著越來越多的資料被上傳至雲端，資料安全及隱私保護也成為各界所關注的重要議題。資料加密是目前確保雲端資料安全性的普遍作法，但資料加解密的過程也會消耗相當大量的系統資源，導致整體服務的效能降低。為解決上述之問題，本研究提出適用於雲端環境下之資料保護架構，以兼顧雲端資料安全及使用效率。本研究所提出之雲端環境下資料保護架構是針對雲端環境安全考量之資料所設計，主要是透過特別設計之隱私保護演算法，先對欲存放之資料屬性，進行機敏性的區分，再依據不同資料的機敏性，分別施以不同強度之資料加密或不加密處理，並分別存放於私有雲或公有雲環境。本研究同時採用美國國防部規範（DoDAF）進行本架構細部之描述。

Abstract

Cloud computing is becoming innovative service model in the world because of high performance of computing and high capacity of storage. However, the security problems are the concern of using cloud computing for enterprise and have become an important issue. Data encryption is a popular method for protection of cloud data. However, the process of data encryption and decryption will consume a lot of system resources which may affect the performance of system service. In this paper, we propose a data protection architecture to balance the performance of system service and protection of data security in cloud environment. In the proposed architecture, the data of enterprise is first classified into high sensitive, low sensitive and unclassified data using a designed privacy protection algorithm. The high-sensitive and low-sensitive are then encrypted using different encryption method and stored in the private cloud and public cloud and leave the unclassified data unencrypted. We also use DoDAF to describe the details of the proposed architecture.

一、前言

網路的發達提高了資料存取的效率，也帶來了資料安全問題。因此，世界各國紛紛制定了許多隱私保護的政策及法律規定，如美國聯邦政府所制定的金融服務法（The Gramm-Leach-Bliley Act，GLB）、醫療保險可攜性與責任法案（Health Insurance Portability and Accountability Act，HIPAA）、電子通訊隱私法（Electronic Communications Privacy Act，ECPA）[7]及我國制定的個人資料保護法[6]等，都對於資料保護的議題加以規範。

自從雲端運算（Cloud Computing）一詞於 2006 年首次被提出來之後，目前已經成為熱門的研究領域，雲端服務所帶來的強大運算能力與儲存容量媲美超級電腦，但是整體建置成本較為低廉，因此，吸引用戶改變原有習慣，使得雲端運算逐漸發展成為一種新的商業營運模式。根據國際資料公司（International Data Corporation, IDC）的調查分

析，雲端運算的服務模式為企業帶來了幾項重要的優勢[1]，包含了隨需求付費、佈署容易、節省資訊設備投資及降低人力成本等等好處。然而，雲端運算也帶來了新的安全問題[2-8]，這些雲端運算專屬的安全問題若不能解決，雲端運算的發展將受到限制[3]。在 iThome[5] 2011 年所提出的調查報告中指出，近 7 成的企業有意願採用雲端儲存服務，但是多以資料備援與非關鍵應用資料為主，一些重要的關鍵系統(如 CRM、ERP 等)內容仍然會考量安全問題，而沒有上傳至雲端。雖然公有雲的租用成本低廉，但其安全性可能有疑慮[9]，如資料的保密性、資料管理的可信度，資料遺失等。因此，企業偏好選擇私有雲作為導入雲端運算的第一步[10, 11]。私有雲的好處是專屬企業使用，雖然其建置成本較高，但資料及服務品質都可以由自己掌握。未來企業選擇雲端的趨勢會朝向混合雲（Hybrid Cloud）發展[12]，因為混合雲可以先由企業建置內部私有雲，再視需求及使用量租用外部公有雲的服務，使得 IT 資源的利用更有彈性。

為了保護雲端資料的安全，目前常採用「資料加密」作法，其是對於雲端儲存環境的資料與檔案全部進行加密後再儲存，待使用者需要取用時再執行解密，所以使用者在資料存取過程中會反覆不斷地執行加密與解密的動作。此方式將會消耗大量的系統資源如 CPU、記憶體等資源，使得系統負擔沉重，大幅降低系統效能[13]。因此，本研究擬提出雲端環境下資料保護架構以解決上述之問題。

本研究所提出之雲端環境資料保護架構是先將雲端資料儲存方式區分為私有雲及公有雲。企業的原始資料先透過本研究所設計的雲端隱私保護演算法處理進行機敏性區分，再依資料的機敏性進行分級加密，分別儲存於私有雲及公有雲，並且對機敏資料進行存取控制，以此減少資料加密的資源消耗，並同時兼顧雲端運算的效能。本文同時利用美國國防部架構規範（DoDAF）進行各個階段的產出文件意涵之描述，以說明本架構之可行性。

本文其餘段落安排如下：第二節說明本研究提出之雲端資料保護架構；第三節為符合美國國防部架構規範（DoDAF）對本研究所提出架構之描述；第四節則是本文的結論。

二、適用於雲端環境之資料保護架構

本研究根據未來企業在雲端可能使用的資料儲存環境，提出雲端資料保護架構，其資料保護方式及資料存取控制分述如下：

1. 資料保護方式

一般而言，從企業角度來看，只要是公開後會對企業造成損失或影響的內容都可以列為高機敏資料，只限於符合認證並擁有權限的內部使用者存取；而屬於與使用者自身相關的資料則列為低機敏資料，則限於符合認證的外部使用者存取；而不具上述機敏性質之資料則屬公開資料，例如企業對外公告的資訊等，則可提供一般使用者瀏覽。在資料儲存方面，可以區分為組織內部的私有雲及外部的公有雲環境。組織內部的私有雲擁有最高的管理自主權，可以完全掌握資料的所有權與控制權，而外部的公有雲環境則是根據其簽訂的服務層級協定（Service Level Agreement, SLA）規定之內容，由雲端環境供應商所代為管理，管理機制由雲端環境供應商所制定，管理自主權相對來說比較低。

本研究所提出之雲端資料保護架構(以下簡稱本架構)即依據上述之概念，將欲保護之資料區分為高機敏性資料、低機敏性資料及無機敏性資料等三大類，並分別將高機敏性資料存放於私有雲內，並施以高強度加密；而低機敏性資料及無機敏性資料則存放於公有雲內，並施以低強度加密及不加密處理，如圖 1 所示。其詳細執行方式如下：

(1) 首先執行隱私保護演算法，移除企業資料庫中機敏欄位的內容，或調整機敏欄位原始值，隱藏其機敏內容，完成欲存放於公有雲之資料。
(2) 欲儲存於公有雲中的資料再透過隱私保護演算法，進一步區分低機敏性及無機敏性的公開內容，分別存放於公有雲
(3) 將已區分為高機敏性之資料則存放於私有雲。

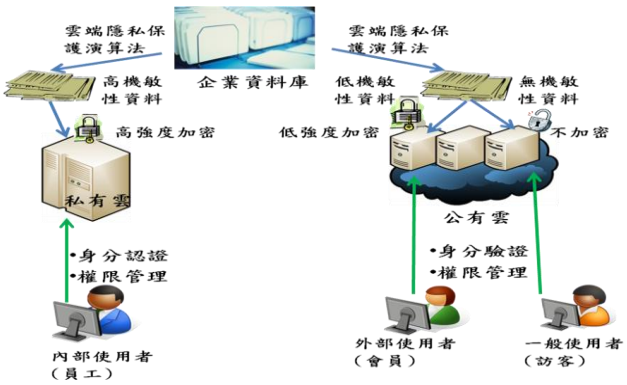

圖 1 本雲端環境資料保護架構示意圖

2. 資料存取控制

本研究將使用者區分為企業的內部使用者（員工）及外部使用者（會員）、一般使用者（訪客）等身份，而連網設備類型可以區分為個人電腦、行動裝置等設備，不同設備規格的差異，會影響到身份認證技術及加密方式的選擇，如圖 1 所示。

由於私有雲存放高機敏性之資料，若這部分資料若洩露，重則影響企業生存，因此，此部分資料僅限內部使用者（員工）進行存取。為保護此部分資料，本架構採用兩種以上的認證技術進行身份驗證，並管制其存取權限；在公有雲的環境下，資料是由雲端供應商代為管理，資料管理機制由供應商所制定，考量雲端處理的資料量龐大，公有雲對於低機敏性資料採用低強度的加密演算法處理後儲存，來減輕系統運算負擔，外部使用者（會員）對低機敏資料進行存取時，可以採用動態密碼（One Time Password, OTP）驗證方式進行身份驗證，並

管制其存取權限。若是用戶使用行動裝置，則增加無線傳輸加密機制(例如 WEP 及 WPA 等)，以保護資料傳輸時的安全。而無機敏的資料則直接儲存於公有雲上，不需額外加密並開放一般使用者(訪客)公開瀏覽及存取。

三、雲端環境資料保護架構描述

為了更進一步說明雲端資料保護架構的運作方式，本文採用美國國防部架構規範（DoDAF）來描述本研究所提出之架構。DoDAF 是一套有效描述國防任務架構或是軍事系統架構之參考與指導，也可以用於非軍事應用。藉由作業（作戰）觀點（Operational View, OV）、系統與服務觀點（System View, SV）及技術標準觀點（Technical View, TV）等觀點來分析描述國防系統運作及流程的整合架構[14,15,16]。透過 DoDAF 規範描述的產品可以執行跨組織的比較與關聯，完整呈現系統的功能。利用 DoDAF 的規範可以更完整地描述本研究提出的雲端資料保護架構的發展、演進及運作方式，建立系統設計規畫的基礎，提供不同領域的人員一個溝通的橋樑。

DoDAF 規範各個觀點之間的關係如圖 2 所示。DoDAF 規範在不同的觀點會產出不同的描述文件，本文參考 DoDAF2.0 規範的 8 種觀點及 52 種描述模式，依據本研究之需要產出計有高階作業概念圖（High Level Operational Concept Graphic, OV-1）、作業節點連接描述（Operational Resource Flow Description, OV-2 ）、組織關係圖（Organizational Relationships Charts, OV-4）及作業活動模式（Operational Activity Model, OV-5b）等描述文件[18]，其意義與目的分別說明如下：

1. 高階作業概念圖（OV-1）

高階作業概念圖是以圖形描繪出全般運作任務，並強調運作任務中主要的作業節點及運作方式，利用不同的圖像及文字說明表現任務中所在位置、組織、資產或目標，提供整個架構的運作概念。本架構的高階作業概念圖如圖 3 所示，本文利用 DoDAF 架構開發工具軟體 IBM Rational System Architect 所繪製，在圖型中以雲端隱私保護架構為核心，其組成包含企業資料庫、私有雲、公有雲及使用者等四個藍色區塊，核心活動流程包含隱私資料保護、分類儲存、分級加密及權限管理等四個紅色區塊。從企業資料庫、私有雲、公有雲及使用者等節點區塊以箭頭指向雲端隱私保護架構代表其節點本架構組成要素，而活動流程方塊與不同節點之間的連線代表活動與節點的關係。例如企業資料庫節點與隱私資料保護和分類儲存兩活動的連線代表企業資料庫的資料會先經過隱私資料保護流程對機敏資料內容加以調整，而調整後的資料再區分機敏性進行分類儲存的動作，私有雲與公有雲兩個節點與分級加密和權限管理兩活動之間的連線代表依據不同機敏等級的資料使用不同等級的加密程序來加以保護，以及透過權限控管的活動來限制使用者存取資料的權限。透過此圖形的描繪讓相關人員對本架構先行產生整體的運作概念。

2. 作業節點連接描述（OV-2）

OV-2 以圖形方式描述具有產生及處理資訊的節點與組織，將各節點之間的資料交換需求以具方向性箭頭（需求線）表示，目的是追蹤從一特定節點至其他節點的資料交換需求，作業節點會隨著層級架構而有不同的解釋，資料交換的內容可以作為架構開發及架構運作之準據。

在本描述文件中，作業活動可以分為八個節點，分別是企業、企業資料庫、私有雲、公有雲、內部使用者、外部使用者、一般使用者及系統管理者，其中包含決策節點、作業節點及使用節點等三種節點類型，決策節點為實線方框代表企業，作業節點為虛線方框代表企業資料庫、私有雲及公有雲，使用節點為雙實線方框代表三種使用者及系統管理者，如圖 4 所示。各節點之間交換的需求如需求線的文字說明，箭頭方向指示從來源端至目的端的需求。決策節點中的項目為企業對於資料保護的相關指導政策，包含使用者存取權限政策、機敏性資料分類政策與資料分級加密政策等，其政策指導會指向企業資料庫、公有雲及私有雲三個節點，控制其節點內活動的執行。而內部使用者、外部使用者及一般使用者三個節點中的活動則對於企業資料庫、私有雲及公有雲等作業節點提出存取的需求，而作業節點在根據權限管理的活動流程賦予權限，系統管理者則對企業資料庫提出存取的需求進行系統管理的工作。

3. 組織關係圖（OV-4）

組織關係圖呈現雲端資料保護架構中企業與組織和公有雲環境、私有雲環境及使用者之間的隸屬關係。組織關係圖如圖 5 所示。在雲端資料保護架構中包含企業、資訊部門、企業資料庫、私有雲、公有雲、雲端供應商等單位，相關人員包含內部使用者（員工）、企業內系統管理員、外部使用者（會員）及一般用者者（訪客）。其中系統管理者、員工、私有雲、企業資料庫隸屬於企業以實線表示，公有雲隸屬於雲端供應商以實線表示，公有雲與企業之間為租用服務的關係以虛線表示，會員及訪客與公有雲之間的關係為需求服務關係以虛線表示。

4. 作業活動模式（OV-5b）

作業活動模式是指在分節特定任務項目中所發生的活動，並在架構中呈現作業行動與行動間的相互關係。本圖採用 Visio 2007 流程圖軟體的 IEF0 圖形來繪製，在系統中的每一個活動以一個方塊表示，於方塊右下角顯示活動的次序及階層符號。活動與活動之間，以箭頭代表輸入、輸出及控制端，箭頭可以用來識別功能流入及流出的方向。圖形中輸入代表執行活動所需的資料，輸出代表執行此功能後所產出的資料，控制端代表此功能如何產生。作業活動模式一般以階層式方式呈現，利用階層化的技術可以將複雜的活動解構化，在活動名稱上方的箭頭為控制端，代表執行活動所依據的政策與規

範，下方為參與單位及工作機制，活動的輸出將成為後續活動的輸入，直到產出最終的輸出結果，透過作業活動模式使我們了解各階層活動的執行情形與前後關係。本架構產出之作業活動模式如圖 6 所示，其活動分述如下：

(1) 隱私資料保護階段：企業資料庫中的原始資料作為輸入源，雲端隱私保護演算法為控制端，輸出為依機敏性分類後資料，並提供作為分級加密及分類儲存兩個活動的輸入源。

(2) 分級加密階段：依機敏性分類後資料為輸入源，受到資料分級加密政策所控制，本活動的執行機制，依據資料機敏性的等級在公有雲及私有雲的環境下執行不同強度的加密動作，其輸出為加密資料。

(3) 分類儲存階段：本活動的輸入源為加密資料，活動受機敏性分類政策所控制，活動的執行機制是將企業資料庫及加密處理的資料依據機敏性分類政策將高機敏資料儲存於私有雲，而低機敏及公開資料則儲存至公有雲。

(4) 權限管理階段：本活動的輸入源為雲端環境儲存之資料，受到使用者存取權限政策所控制，活動的執行機制是在公有雲及私有雲環境下對使用者進行身份驗證後，使用者再根據被賦予的權限存取資料，活動輸出為授權存取的資料。

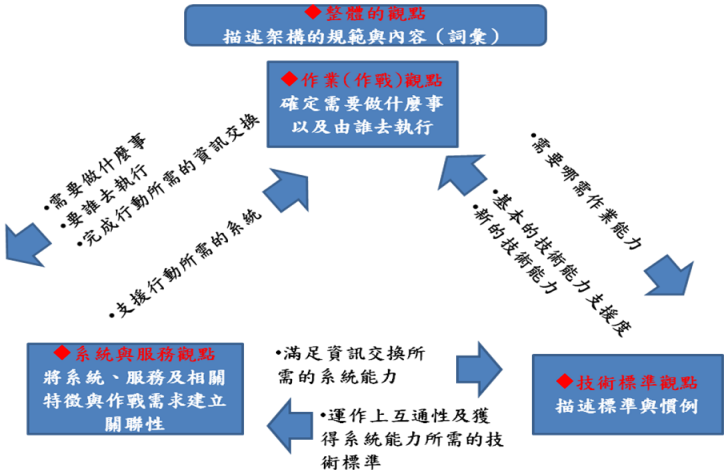

圖 2 DoDAF 觀點關聯圖[17]

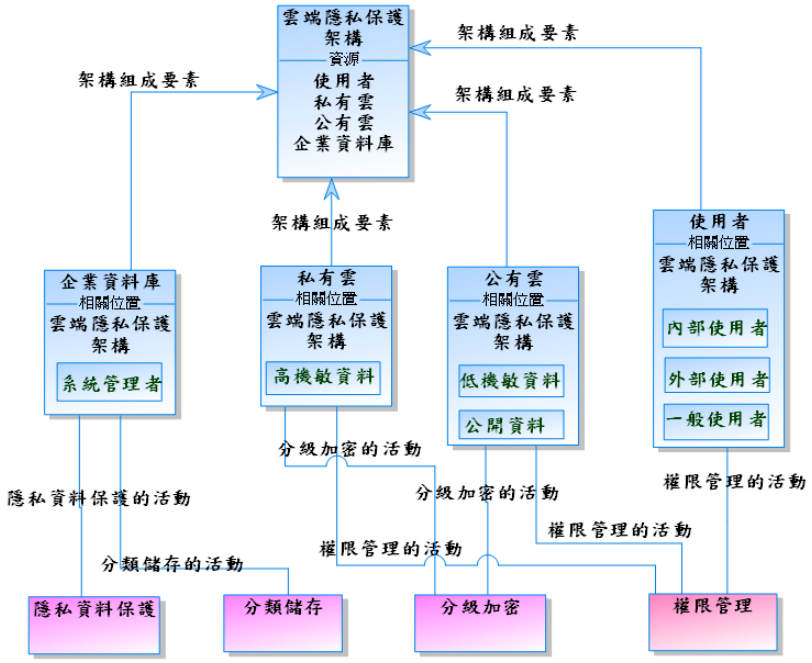

圖 3 本架構之高階作業概念圖(OV-1)

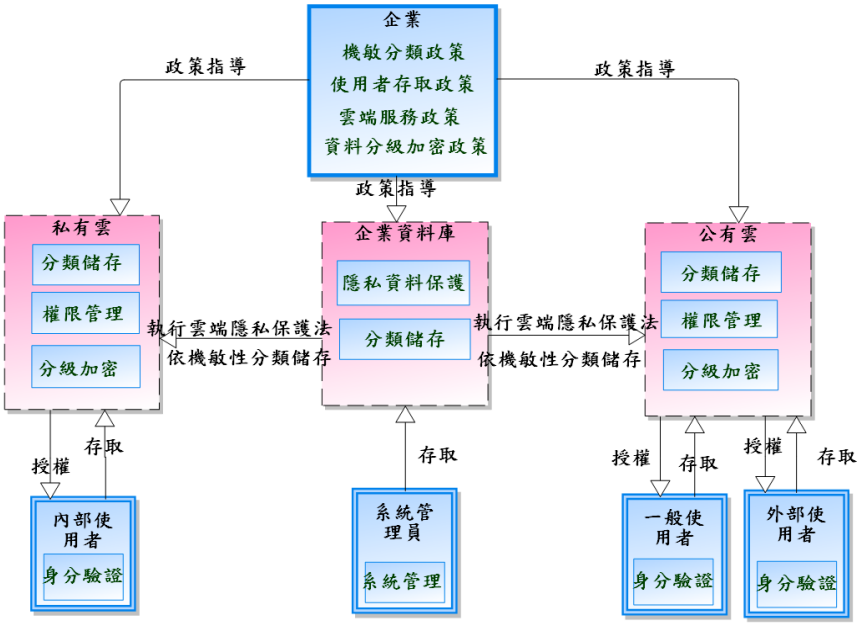

圖 4 本架構之運作節點連接描述(OV-2)

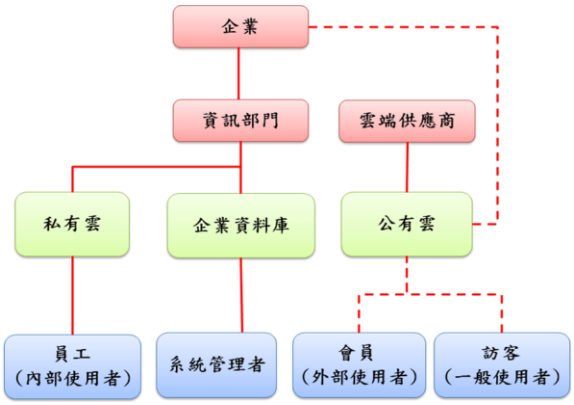

圖 5 本架構之組織關係圖(OV-4)

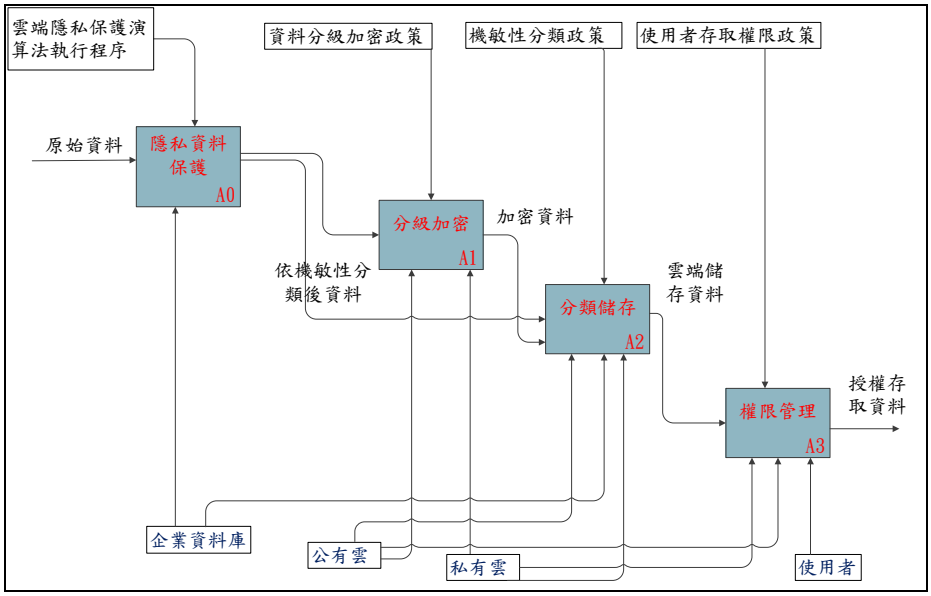

圖 6 本架構之作業活動模式(OV-5)

四、結論

由於資料加解密的過程會消耗相當大量的系統資源，導致整體服務的效能降低。本研究提出適用於雲端環境下之資料保護架構，以兼顧雲端資料安全及使用效率。

本架構將欲保護之資料區分為高機敏性資料、低機敏性資料及無機敏性資料等三大類。對高機敏性資料而言，將其存放於私有雲內，施以高強度加密及採用兩種以上的認證技術進行身份驗證。對低機敏性資料及無機敏性資料而言，則將其存放於公有雲內，並對低機敏性資料施以低強度加密及採用動態密碼驗證方式進行身份驗證；另外，增加無線傳輸加密機制，以保護資料使用無線傳輸之安全。

本文同時嘗試使用 DoDAF 規範所產出的文件產品描述所提出的雲端資料保護架構，產出包含高階作業概念圖(OV-1)、作業節點連接描述(OV-2)、組織關係圖(OV-4)及作業活動模式(OV-5b)等文件從不同的觀點描述同一架構，讓不同領域的人員可以更為瞭解本研究架構於各個節點與各個活動之間的運作流程，對於後續完成雲端資料保護架構的目標將有所助益。

後續將對於本架構在技術層面的隱私保護演算法、分級加密程序及權限管理領域加以深入研究與設計，以期實現雲端環境下資料保護架構具體化的目標。

五、參考文獻

[1] https://www.eiseverywhere.com/file_uploads/86cde4f4bf015bb8cd2153ea7e0287ff_Day_1_815am_Frank_Gens_Bringing_Cloud_into_the_Enterprise.pdf(2009)

[2] http://download.microsoft.com%2Fdownload%2F3%2F9%2F1%2F3912e37e-5d7a-4775-b677-b7c2baf10807%2Fcloud_privacy_wp_102809.pdf (2009)

[3] C. L. Liu, W. H. Chen, and D. K. Tung, "Identification of Critical Security Issues for Cloud Computing," *Applied Mechanics and Materials*, Vol. 145, pp. 272-276, 2012.

[4] S. Childs, and A. Dayley, *Organizational Collaboration and the Right Retention Policies Can Minimize Archived Data and Storage Demands*, Gartner report, 2012.

[5] http://www.ithome.com.tw/itadm/article.php?c=65622&s=6(2011.1.24)

[6] http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=I0050021(2010.5.26)

[7] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and Privacy in Cloud Computing: A Survey," 2010 Sixth International Conference on Semantics Knowledge and Grid (SKG) , Shanghai, China, pp.105-112, 2010.

[8] Y. Tan, and X. Wang, "Research of cloud computing data security technology," 2012 2nd International Conference on Consumer Electronics Communications and Networks (CECNet), pp. 2781-2783, 2012.

[9] 紀博文，"資料在雲端？談雲端儲存的安全性議題"，資安人雜誌，台灣，No.79，pp.39-45，2011。

[10] http://zppleweb.wordpress.com/2010/11/23/gartner-says-it-organisations-will-spend-more-money-on-private-cloud-computing-investments-than-on-offerings-from-public-cloud-providers-through-2012(2010.11.23)

[11] http://www.vmware.com/tw/company/news/releases/vmw-CTO-2011-2-1-2012.(2012)

[12] http://easystreet.com/wp-content/uploads/2011/12/Gartner_The-Road-Map-From-Virtualization-to-Cloud-Computing-G00210845_English.pdf (2011.12)

[13] I. H. Chuang, S.H. Li, K.C. Huang, and Y.H. Kuo, "An effective privacy protection scheme for cloud computing," 2011 13th International Conference on Advanced Communication Technology (ICACT), pp.260-265, 2011.

[14] S. Matin, "Using System Architecture Maturity Artifacts to Improve Technology Maturity Assessment," *Procedia Computer Science*, vol. 8, pp.165-170, 2012.

[15] Chief information officer, *DoDAF Architecture Framework Version 2.0 Volume I：Manager's Guide Introduction, Overview, and Concepts*, U.S.DoD, Washington D.C., 2009.

[16] 徐禮睿，建立國軍合約管理教育訓練之研究：DoDAF規範之運用，碩士論文，國防大學管理學院運籌管理學系，台北，2012。

[17] X. Zhang, "The Process of information System Architecture Development," *Procedia Engineering*, Vol.29, pp.755-779, 2012.

[18] 王鎮胤、韓孟麒、王正航，運用DoD AF導入C4ISR系統指管流程之研究－以防禦海軍艦隊預警雷達程序為例，第十四屆國防管理暨實務研討會，台北，第1-13頁，2006。