福祉科技與服務管理學刊
Journal of Gerontechnolgy and Service Management

研究計畫

智慧型醫療照護雲端系統之建置研究

張瑞雄[1] *彭勝龍[2]
[1]國立台北商業大學 資訊與決策科學研究所
[2]國立東華大學 資訊工程學系

摘要

在一套完整的居家照護系統中，無論是影像辨識或巡航監控，甚至是環境感測與行為警示技術，均需要即時且大量的運算，此特徵正符合巨量資料的標準，即為速度(velocity)、資料量(volume)以及資料多元性(variety)；因此，為了能讓各種系統與設備順利運行並有效降低系統複製成本，使用雲端運算技術絕對是勢在必行；此外，將居家照護系統連接上雲端的優勢更遠大於使用本地設備，例如歷史資料的安全性與可靠性、彈性且可輕易擴充的運算能力，以及分析歸納監測資訊以達到判斷當前狀態與預測未來發展可能性；然而迴異於一般雲端運算架構的部分，在於各個系統間的資訊收集與運算結果必須達到共享與同步，因此如何能建立一個協同各系統調控與計算結果的雲端運算系統將是個重大的挑戰。

本計畫將針對異質性系統間的資料，進行處理以及資料的傳遞與同步，研發各種應用程式介面與運算模型，而工作項目包含有建立硬體設備、資料檢索平台、運算模型與加密技術，並繼續研讀最新的運算技術資料用以精進本計畫之運算效能，維持雲端計算性能的擴充性。

關鍵詞：健康照護、巨量資料、雲端運算

1. 本研究計畫之背景、目的、重要性

根據內政部統計，截至 2013 年 7 月底，國內扶老比為 15.3%、人口老化指數為 78.3%，都較前年同期大幅增加，國內領有身心障礙手冊者已近 112 萬人，10 年來增加了 29 萬人，兩種數據都顯示國內長期居家照護的人力需求逐漸向上攀升。但觀目前我國對長期照護服務的投入仍舊不足，社會福利與健保制度的可照護範圍也十分狹小，提供服務的人力與設施亦嚴重欠缺，導致絕大多數長期照護的責任均由家庭獨力負擔，造成沉重的身心與財力負荷。

為了因應上述的問題，國內各大醫療院所推出各項遠距照護計畫，IT 廠商也無不積極規劃遠距健康照護領域的運籌策略，透過科技的應用，有效的減少因照護所花費的人力與時間；然而目

*通訊作者：rschang@ntub.edu.tw

前各種生醫感測裝置或閘道器大多採用有線且固定式的方式收集感測資訊，並且零散的提供感測資訊而非整合管理，除了在使用上的不便，也無法妥善的儲存與監控各項資訊。本計畫導入雲端運算的觀念，以「醫療雲」的基礎構想延伸，發展為「照護雲」的主要功能與架構，希望偏遠地區的民眾或是老年人在家亦可獲得妥善的醫療監測；遠距居家照護包含：生理狀況監測、復健照護及緊急醫療救護等，透過整合的運算與存儲資源，提供老年人更符合需求的服務與照顧。

然而由於需要進行多種的生理資訊監測，使用者的隱私保護便更加重要。例如透過監測攝影機可以得知使用者正在做什麼事情，這對於使用者的隱私可能產生相當大程度的侵犯，因此在架設「照護雲」時，需要採用私有雲與公有雲混合的機制，使用者被監測的記錄送往私有雲進行判斷，若發現數據不正常，私有雲將直接送出求救的訊息到緊急救護雲中，通知救護車或家人進行救護，同時在私有雲中亦可加密使用者過往的記錄資料，讓使用者的生命記錄更加地有保障。

1.1 雲端運算(cloud computing)

隨著網際網路的發展，其電腦的運作方式也已逐漸的被改變，透過這種雲端的網際網路運作方式，共享的軟硬體資源和訊息可以按需求提供給所需的電腦或者其他智能產品裝置。而雲端運算有幾項簡單的特徵：

- 隨使用者需求應變自助服務
- 隨時隨地用任何網路裝置存取
- 多人共享資源池
- 快速重新部署靈活度
- 可被監控與量測的服務
- 基於虛擬化技術快速部署資源或獲得服務
- 減少使用者終端的處理負擔
- 降低了使用者對於 IT 專業知識的依賴

而其服務的模式共有三種：

- 軟體即服務(SaaS)：消費者使用應用程式，但並不掌控作業系統、硬體或運作的網路基礎架構。
- 平台即服務(PaaS)：消費者使用主機操作應用程式。消費者掌控運作應用程式的環境（也擁有主機部分掌控權），但並不掌控作業系統、硬體或運作的網路基礎架構。
- 基礎架構即服務(IaaS)：消費者使用「基礎運算資源」，如處理能力、儲存空間、網路元件或中介軟體。

將雲計算帶入本計畫的原因是可以整合其他獨立性高的相關計畫，透過一個共通的平台，提供 web service 的方式給使用者去使用，而這平台也必須提供各個相關計畫內的系統架構儲存資料、分析比對資料，並且提供各個相關計畫所需要大量且快速的計算，在這部分雲端技術可以充分的提供。

1.2 資料視覺化(data visualization)

近幾年來，隨著電腦的廣泛運用以及網路的快速發展，各式各樣的資料也累積的越來越多，如何從這些巨量資料中找到有用的資料，並以簡易的方式呈現讓使用者一目了然，儼然也成為了當下的熱門議題之一；資料視覺化的基本概念是將每一筆資料當作圖像的最小元素，當巨量的資料彙整在一起就構成一個數據圖像，便能觀察其變量。

所以如果能將很繁雜且制式化的數字以視覺化的方式在我們的雲端平台上呈現，對使用者來講會方便許多，因為當我們想探勘巨量資料的情況下，能以幾條曲線甚至幾張簡單的圖表就能夠看出其資料的差異或變異性，如此對於使用者來說，了解自己身體近期（月/年）的變化是多麼的方便。況且，這種將資料視覺化的方式也能夠很快的讓使用者去分析比對過往之歷史資料，幫助使用者在進行資料分析的時候可以更有效率和節省更多的時間。

1.3 雲端加密機制(cloud encryption)

利用上述雲端技術建立完成醫療雲服務之後，所有的相關計畫資料都會上傳至雲端上儲存，與此同時，當資料交由第三方保管時就會產生隱私的問題，第三方也就是雲端服務的提供者，要如何確保資料的完整性與隱私性是現在雲端科技發展的一項非常重要之課題。

Homomorphic Encryption 是一項近年來十分熱門的全新加解密技術，它的概念是先將資料加密之後再將資料上傳到雲端，給雲端去做運算，等結果運算完成之後再自己解密，整個過程中，雲端的提供者只是針對一串密文去做運算，如此，雲端的提供者便完全無法得知使用者所上傳的資料內容，也就是說，我們資料的隱私權可以得到充分保護。再將這套技術引入本計畫的內容中，即可完善的保護使用者各項醫療數據的隱私權，並且妥善的保護各相關計畫間的資料不會外露。

2. 國內外有關本計畫之研究情況、重要參考文獻之評述

2.1 Application of cloud computing in the health information system

隨著雲端運算越來越成熟，所有由雲端運算提供的產品都能視為一項服務，而雲端運算也是一種新的商業模式，衝擊著整個 IT 產業，IT 將作為往後的一項服務，使用其服務需要付其一定的費用。人的一生大概可以分成四個階段，生、老、病和死，這也是為什麼醫療和健康一直以來都被全球所重視，近幾年來更是被密切的關注，但是人的生命是無價的，醫療資源是有限的，我們如何將有限的醫療資源做最有效的利用呢？採用雲端運算建立一個分享和交流的醫療資訊平台，提供健康保健的服務（如圖 1），是一種有效的方式來協調醫療服務，而不用在架設基本的平台，而不同的醫療單位也可以使用這個平台，可以節省一筆花費，也能充分利用這個平台。並幫助一些農民實現小病在村莊內就能治療，不必再跑到城市就醫，來減少看醫生太困難或太貴的困擾，當務之急是使用雲端運算建立一個健康資訊系統。

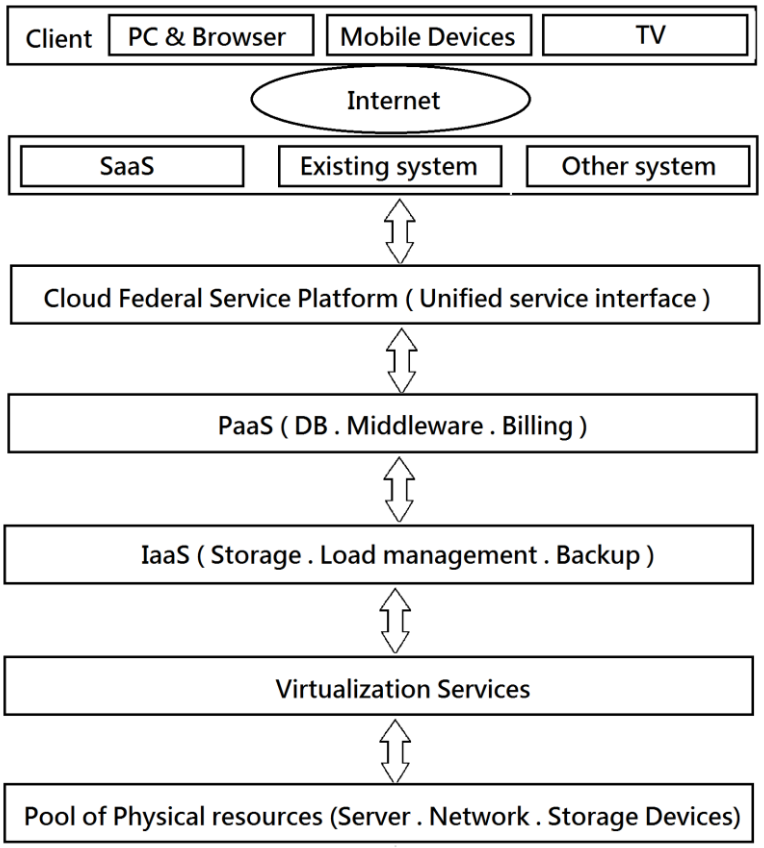

圖 1. A basic structure of health information system

2.2 Cloud-based e-health multimedia framework for heterogeneous networks

因為醫療資料有著許多不同的紀錄型態，其中有影像、視頻、音頻、數位信號以及文字資料。而當資料傳送進入後要進行儲存必須先進行過處理，因此在此會透過生物訊號將需要的部分進行計算，最後利用高頻寬轉送接收，將處理過的病人資料到雲端的儲存裝置中。另外，在進行生物訊號運算時會消耗實體資源也就是應用程式的伺服器，原因是因為必須從雲端下載資料，因此 CPU 和 Memory 的資源成本是不可避免的。

以雲端的機制進行資料搬移和傳遞，但資料卻來自於各種不同的設備裝置上，而所使用到的設備很多都來自於各種影音設備，他們錄下的病人數據都需要經過編碼解碼影音檔才比較容易在不延遲和不遺失的情況下有效地進行傳輸和應用，我們也使用多種不同的家中設備進行醫療性質的監測工作，家庭中的影音設備和監測設備所得到的數據資料較不會是非常複雜難以處理的型態。因此，若在所架設的整體系統上進行運作，可以得到不錯的運作效果，但有大部分是在講述影音解碼編碼的處理，因此架構中有很大一部分著重在影音處理傳輸部分，雲端系統的架構最主要在提供部分資料計算以及資料和儲存設備間傳送情形，所以提供較多之雲端內部資料的移動和傳輸，為了容易操作，因此必須另外加上符合使用者可以方便操作的 API 以及儲存介面才能比較符合我們的計畫目的（如圖 2）。這方面的研究如(Chowdhury et al., 2010; Nkosi & Mekuria, 2010; Mekuria et al., 2010; Archer et al., 2011; Zheng et al., 2012; Hsu et al., 2012)。

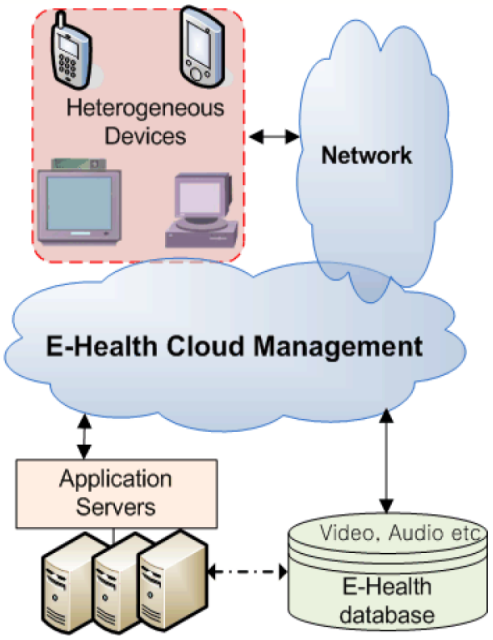

圖 2. Framework for e-Health application in cloud computing functioning over heterogeneous networks and devices

2.3 Research on visualization techniques in data mining

視覺化的資料探勘可以幫助處理巨量資料，而這項技術的優點在於可以讓使用者直接參與資料探勘的過程，而根據視覺化資料分析的結果，使用者可以直接用不同的資料探勘演算法再加以專業醫療方面的知識整合，最後得到最適合使用者的資料型式展示給使用者去分析比對(Muller et al., 2011; Ganesh et al., 2012)。

資料視覺化的目的主要是設計與選擇適合的展示方法去呈現多筆資料間彼此的關係，讓使用者可以很快的將資料進行圖像化的分析。此外，也進行分析比較傳統的視覺化技術方法與較新的視覺化技術，傳統方法如 Visualization Methods Based on Geometric Projection Technology、Image-Based Visualization Technology、Pixel-Oriented Visualization Methods 及新的視覺化技術如 Distortion Techniques、Interactive Technologies and Collaborative Technologies、Drill-Through Technology 及 Virtual Technologies 等。

2.4 Data processing and presentation for a personalized image driven medical graphical avatar

隨著醫療行業的數位化，導致各種類型的醫療資訊大幅增加，例如影片、照片和各類觀測紀錄，患者常常在看診之後會收到大量資訊，但是這些資訊大多都是以最簡單的方式，例如純文字的病歷或是沒有任何解釋的圖片，現有的個人健康紀錄系統(current personal health record systems, PHR)，雖然能夠整合儲存患者的各項醫療相關數據，卻無法讓患者方便的了解和管理這些資訊，原因在於一般的圖像和影片無法讓人一目了然，對沒有足夠專業知識的患者而言，每個訊息幾乎都是獨立的，並沒有關連性，缺乏一種容易瞭解的圖形化方法。

本篇提出了一個從患者自身建立的全身醫療圖像(medical graphical avatar, MGA)。如圖 3，在 MGA 系統接收到醫療訊息時，首先會先判斷資料的類型，資料分別為圖片、影片和雜項，檔案類行為影片格式，就會在檢查檔案是否有註解，並將其提取出來；如果是圖片檔，當系統判斷是圖片為 PET-CT（正子電腦斷層造影）就可以開始分段建立 3D 模型，一般的圖片檔案則利用 ROI 將重要的部分框選出來，如果資料中都沒有任何想要的資訊，還是會記錄並且編列到時間軸裡面，以利往後方便瀏覽。最後建立的 3D 模型可利用 HTML5 和 WebGL 提供網路上的瀏覽。

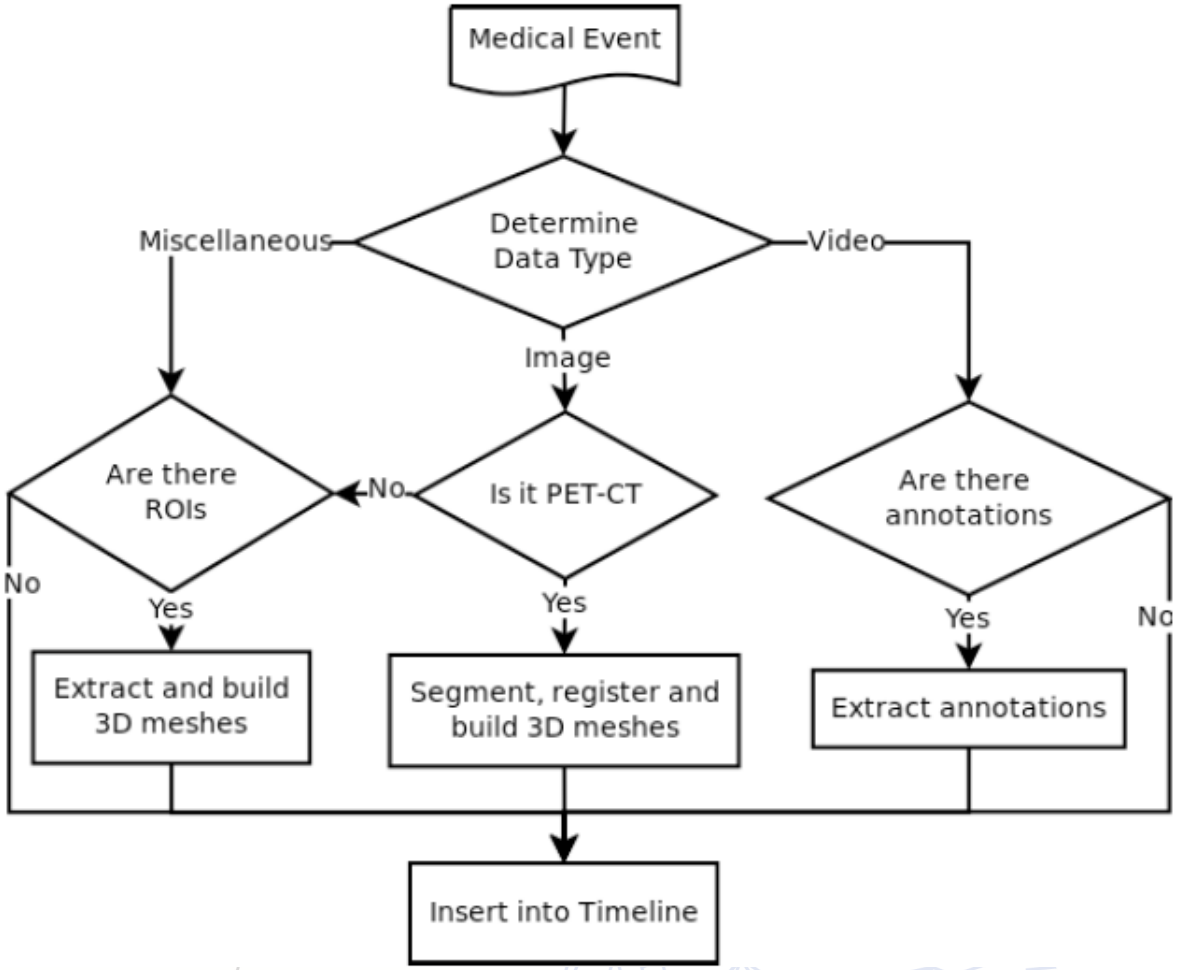

圖 3. High level overview of MGA system

健康照護是一個長期性的觀察行為，長久下來一定會累積種類繁多又大量的資料(Lobodzinski, 2011)，MGA 系統可以把不同格式的資料做整合並且排序，提供醫療事件的歷史資料查詢表單，透過時間軸來觀察數據的變化也方便使用者理解資料所帶來的意義。使用 ROI 可以針對重點部分額外擷取出來，做細部觀察，而且圖片所建立的 3D 模型可使用 HTML5 和 WebGL，方便我們整合到網頁，使用一般的瀏覽器就可以觀看，不需要額外安裝程式。

2.5 Assessment of cloud-based health monitoring using homomorphic encryption

為了有更好的預防疾病的方式，已經將醫療保健推進數位領域，利用雲端計算來改善病人的監測系統。我們提出了一個新的存取方法用來分析和顯示病人的健康訊息。提出的系統最主要的核心在於將全部的計算工作負載移至雲端當中，但是將病人的隱私資料儲存在雲端中就必須要能夠確保隱私資料的保密性。我們可以利用現有的加密技術來對資料加密，然而在利用雲端處理資料計算時（資料須先解密），病人的隱私資料就會有曝露的危險性。在此利用了全新的加解密技術(fully homomorphic encryption)來對資料做保密(Brakerski et al., 2012; Brakerski & Vaikuntanathan, 2011; Brakerski & Vaikuntanathan, 2014; Coron et al., 2011; Gentry & Halevi, 2011; Gentry & Halevi, 2011)，它允許直接使用加密過的資料做計算，所以不需要將未加密的資料傳送到計算節點上，如此一來可達到病人的隱私資料的保密性，不會讓計算節點（雲端提供者）得知。

我們所提出的系統在此分成了三種階段來執行(如圖 4)，分別是採集(acquisition)、儲存(storage)、計算(computation)。

- 採集：透過一次性的設備來收集醫療資料，並利用 AES 加密技術(Gentry et al., 2012)加密資料後以無線傳輸方式傳送至雲端儲存。
- 儲存：醫療資料允許被儲存在雲端中供往後使用。
- 計算：在進行資料計算之前，資料必須先從 AES 加密轉換成 FHE 機加密才可以進行處理。

資料處理分析完畢後是呈現 FHE 加密格式並將其送至 GUI 設備（行動裝置），透過 GUI 設備進行解密才可以提供醫生（或用戶）了解並診斷用。另外，我們所提出的系統是利用雲端資源來做長期的健康監測，並且可以讓用戶可以透過行動裝置來存取資訊，最重要的是同時能夠確保完整的病人資料隱私。

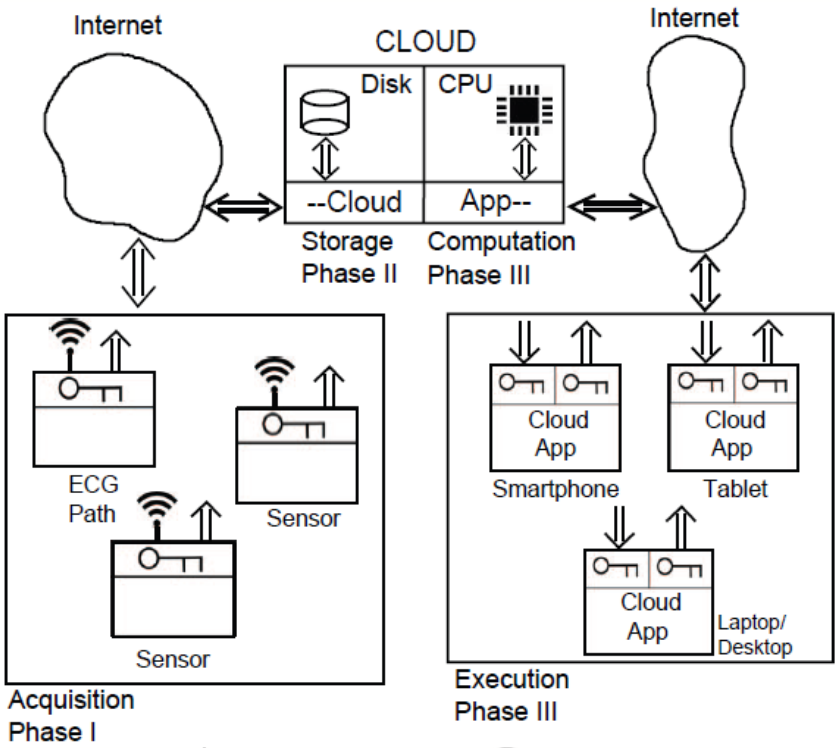

圖 4. Proposed system for long term health monitoring through a cloud-based application

參考資料

1. Chowdhury, A., Chien, H. C., Khire, S., Fan, S. H., Tang, X., Jayant, N., & Chang, G. K. (2010). Next-generation E-health communication infrastructure using converged super-broadband optical and wireless access system. In *world of wireless mobile and multimedia networks (WoWMoM), 2010 IEEE international symposium on a*, 1-5. doi:10.1109/WOWMOM.2010.5534984
2. Nkosi, M. T., & Mekuria, F. (2010). Cloud computing for enhanced mobile health applications. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*, 629-633. doi:10.1109/CloudCom.2010.31
3. Mekuria, F., Nkosi, M., Seotlo, V., & Twala, B. (2010). Intelligent Mobile Sensing and Analysis Research Network in South Africa–Building a base at the CSIR.
4. Archer, N., Fevrier-Thomas, U., Lokker, C., McKibbon, K. A., & Straus, S. E. (2011). Personal health records: a scoping review. *Journal of the American Medical Informatics Association*, *18*(4), 515-522. doi:10.1136/amiajnl-2011-000105
5. Zheng, W., Dong, W., Chen, X., & Zhang, J. (2012). Semantic extraction and processing of medical records for patient-oriented visual index. In *SPIE Medical Imaging*, 831910-831910. doi:10.1117/12.911044
6. Hsu, W., Taira, R. K., El-Saden, S., Kangarloo, H., & Bui, A. A. (2012). Context-based electronic health record: toward patient specific healthcare.*Information Technology in Biomedicine, IEEE Transactions on*, *16*(2), 228-234. doi:10.1109/TITB.2012.2186149
7. Muller, H., Maurer, H., Reihs, R., Sauer, S., & Zatloukal, K. (2011). Adaptive visual symbols for personal health records. In *Information Visualisation (IV), 2011 15th International Conference on,*

220-225. doi:10.1109/IV.2011.87

8. Ganesh, S., van Schie, H. T., de Lange, F. P., Thompson, E., & Wigboldus, D. H. (2012). How the human brain goes virtual: distinct cortical regions of the person-processing network are involved in self-identification with virtual agents.*Cerebral Cortex*, *22*(7), 1577-1585. doi:10.1093/cercor/bhr227
9. Lobodzinski, S. S. (2011). Subcutaneous implantable cardioverter-defibrillator (S-ICD). *Cardiology journal*, *18*(3), 326-331. doi:10.5603/CJ.2012.0039
10. Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2012). (Leveled) fully homomorphic encryption without bootstrapping. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, 309-325. doi:10.1145/2090236.2090262
11. Brakerski, Z., & Vaikuntanathan, V. (2011). Fully homomorphic encryption from ring-LWE and security for key dependent messages. In *Advances in Cryptology–CRYPTO 2011*, 505-524. doi:10.1007/978-3-642-22792-9_29
12. Brakerski, Z., & Vaikuntanathan, V. (2014). Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal on Computing*, *43*(2), 831-871. doi:10.1109/FOCS.2011.12
13. Coron, J. S., Mandal, A., Naccache, D., & Tibouchi, M. (2011). Fully homomorphic encryption over the integers with shorter public keys. In*Advances in Cryptology–CRYPTO 2011*, 487-504. doi:10.4028/www.scientific.net/AMR.989-994.4326
14. Gentry, C., & Halevi, S. (2011). Fully homomorphic encryption without squashing using depth-3 arithmetic circuits. In *Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on*, 107-109. doi:10.1109/FOCS.2011.94
15. Gentry, C., & Halevi, S. (2011). Implementing gentry's fully-homomorphic encryption scheme. In *Advances in Cryptology–EUROCRYPT 2011*, 129-148. doi:10.1007/978-3-642-20465-4_9
16. Gentry, C., Halevi, S., & Smart, N. P. (2012). Homomorphic evaluation of the AES circuit. In *Advances in Cryptology–CRYPTO 2012*, 850-867. doi:10.1007/978-3-642-32009-5_49

A study of implementing an intelligent healthcare cloud system

Chang, R.-S.[1], *Peng, S.-L.[2]
[1] Institute of Information and Decision Science, National Taipei University of Business
[2] Department of Computer Science and Information Engineering, National Dong Hwa University

Abstract

In a complete home care system, whether it is image recognition, cruise control, even environmental sensing and act warning technologies requires immediate and large amounts of computation; this feature satisfies the three V's of big data, which are "Velocity", "Volume" and "Variety". Therefore, in order to allow a variety of systems and equipment running smoothly and reduce the system cost of reproduction effectively, using cloud computing technology is absolutely imperative. In addition, for home care system, the advantage of cloud connected is better than using local equipment, such as security and reliability of the historical data, flexible and easily scalable computing capacity, and analyzing the information of monitoring in order to evaluate the current status and predict the possibilities of development. However, different from the general architecture of cloud computing is that information collection and calculation results of the various systems must be shared and synchronized. Consequently, how to establish a heterogeneous cloud computing system to regulate every sub-system will be a major challenge.

This project is going to focus on data transmission and synchronization in heterogeneous cloud system to develop various API and computing model. Our works include the establishment of hardware, information retrieval platform, computing models and encryption technologies. Furthermore, we still continue to study the latest technical documents to improve our computing performance and scalability.

Keywords: healthcare, big data, cloud computing