# 東海大學資訊管理研究所

# 碩士學位論文

## 應用身分認證技術於物聯網之個人健康紀錄

## Applying a Secure Authentication Protocol of Personal Health Record System in IOT Environment


指導教授：陳澤雄 博士

劉嘉惠 博士

研 究 生：葉 嶸 撰


中華民國 107 年 07 月

# 東海大學資訊管理學系碩士學位

# 考試委員審定書

資訊管理學系研究所 葉嶸 君所提之論文

應用身分認證機制於物聯網之個人健康紀錄

經本考試委員會審查，符合碩士資格標準。

學位考試委員會 召集人：吳鎮宇 (簽章)

委 員：黃愉閔

陳澤龍

劉嘉惠

陳澤雄

中 華 民 國 107 年 7 月 4 日

# 誌謝

不知不覺又來到六、七月了，屬於畢業的季節，也表示已經到了碩士學程的尾聲了。回想起剛進東海的那種不知所措，以及對自己的沒信心，或是對未來的迷茫，但是人生就是這樣，總是會經歷許多挑戰與磨練。有時候萬事起頭難，當我一步一腳印的走過來，只要努力不放棄，終究是可以跨越終點的，而且整個過程與結果都是這麼令人值得回味的。

回首這兩年，我要感謝我的指導老師陳澤雄博士與劉嘉惠博士，老師們不只是對學業上的教導，私底下也非常關心學生的生活，不管有任何困難、想法、或是陷入人生的低潮，都會非常樂意與老師分享，而老師也總是很適時地給予寶貴的意見，這些對我實在是受益良多。也非常謝謝整體雄哥大家庭的同學們，在我這兩年的研究生涯中幫了我非常多的忙，而老師也常常教導我們要熱心並且幫助他人，我們整個大家庭也都時常謹記老師的教誨，甚至以後在社會上也不會忘記這份熱忱的。能夠遇到老師與同學們是我的榮幸，也是一個最棒的緣分，而我也相信這份緣分即使離開學校也會一直持續下去的，在往後的日子裡，那些曾經幫助過我的人都將謹記在我心裡。

口試當天雖然很緊張,但還是順利的通過了,非常感謝口是委員吳鎮宇老師、陳澤龍老師以及黃愉閔老師們提供的批評指教與寶貴意見，有了這些建議才能使我的論文更加豐富與完整。

最後必須感謝我的家人，父母、兄弟還有身邊的好朋友們，我曾經一度想要放棄，如今我能夠完成這個生涯的里程碑都是因為一直有你們在身邊支持我。經歷了這些寶貴的經驗，相信往後的日子裡，我能更有自信、更有能力的迎接未來的冒險與挑戰。

葉　嶸　謹誌

民國 107 年 07 月

論文名稱：應用身分認證技術於物聯網之個人健康紀錄
校所名稱：東海大學資訊管理學系研究所
畢業時間：2018年07月
研究生：葉嶸　　指導教授：陳澤雄
劉嘉惠

論文摘要:

近年來不斷提倡以病人為中心的個人健康紀錄系統，其目的為長期的個人紀錄與改善健康計畫，結合已經成熟的生理感測裝置能夠建置物聯網環境下的個人健康紀錄系統，快速的蒐集個人資訊並傳到後端做保存與日後的存取，然而在物聯網的環境下，訊息的傳遞過程更為開放，比起以往的線路更容易被不法人士竊取身分或是在傳遞過程便將資料攔截進而偷取患者本身的醫療紀錄、醫療機構、以及照護人員等相關資料，因此這樣的架構若缺乏一個有效的安全性機制，將會無法得到使用者的信任，並大大的影響系統使用上的疑慮，並無法達到長期健康計劃的推行與品質。為了確保使用者的重要隱私能被保護，不被有心人士惡意攻擊、甚至竊取，必須確保擁有者有完全的權限去管理自己的個人健康紀錄以及管理授權給其他使用者的權限之開放程度。因此一個安全的身分認證機制能保證只有合法的使用者能登入系統，並通過驗證取得系統服務資源。

本論文針對物聯網環境下的個人健康紀錄系統，提出一個具安全性與隱私性的使用者身分認證機制，讓相關醫護人員長期調閱使用者的健康資訊，並協助做長期的健康照護計劃。此機制是使用通行碼結合專屬的智慧卡的雙重認證機制，讓擁有者以及被授權的使用者能夠登入系統並存取相關的個人紀錄。本研究採用雙線性配對加密系統(Cryptosystem Based on Bilinear Pairing)來雙向驗證使用者的身分，以有效防止惡意的入侵與竊取行為。

關鍵字: 個人健康紀錄、物聯網、身分認證、智慧卡、雙線性配對

Title of Thesis：Applying a Secure Authentication Protocol of Personal Health Record System in IOT Environment
Name of Institute: Tunghai University, Graduate Institute of Information Management
Graduation Time：（07／2018）
Student Name：Yeh, Jung　　Advisor Name：Chen, Tzer-Shyong
Liu, Chia-Hui

Abstract:

Patient-centered personal health record systems are promoted in past years, aiming to permanently record personal physiological conditions and health improvement plans. The combination with a mature physiological sensing device could establish personal health record system in the Internet of Things environment to rapidly collect personal information which is transmitted to the back-end for reservation and future access. Nevertheless, the transmission of information is opener under the Internet of Things environment. In comparison with past routes, the identity can be more easily stolen or data are intercepted in the transmission process to further steal patients' medical records and relevant data of medical institutions and health care personnel. Without an effective security mechanism, the users would not trust such a structure to largely affect the use of the system as well as the promotion and quality of long-term health plans. To protect users' important privacy from hostile attack and even stealing, the owners should have complete authority to manage personal health records and authorize other users. Such a secure identity authentication mechanism could guarantee that merely legal users could log in the system to acquire the system service resources.

Aiming at personal health record system under Internet to Things environment, a user identity authentication mechanism with security and privacy allows medical personnel permanently retrieving the user's health information and assisting in long-term health care plans. With double authentication mechanisms of password and exclusive smart card, the mechanism allows the owners and the authorized users logging in the system and accessing relevant personal records. The use of cryptosystem based on bilinear pairing for two-way user identity authentication could effectively prevent from hostile invasion and stealing behaviors.

KeyWords: Personal Health Record, Internet of Thing, Identity Authentication, Smartcard, Bilinear Pairing

# 目錄

頁次

# 表目錄

頁次



# 圖目錄

頁次

# 第一章 緒論

## 第一節 研究背景

隨著時代的進步與發展，各級醫療院所已經將傳統紙本記錄的病歷轉型為電子病歷(Electronic Medical Records，EMR)[1]系統為主要記錄方式。有了電子病歷，即可長期紀錄與保存個人的醫療資訊，包括個人的健康狀態以及所接受過的醫療照護等，通過驗證授權的醫護人員能夠即時的存取醫療紀錄做新增、修改、或是病歷交換等，但雖然早已有許多院所轉換為電子病歷，但目前的系統較著重於病歷的管理與傳輸上效能上，在交換病歷的階段上雖有許多架構與方法陸續提出，但仍然沒有一個普及被接受的標準，因此各醫療院所之間要如何達到完全的互通性(Interoperability)仍是一個重要的議題。此外電子病歷的主要範疇仍是以提供專業醫護人員做臨床醫療為主要內容，並非以患者長期的健康照護與管理的角度來思考。伴隨著許多資訊基礎科技的完善與普及化，加上近來患者對本身健康照護的自主意識提升，現階段除了許多臨床診斷的醫療研究之外，已經開始透過新的資訊科技與醫療資訊系統所提供的服務，衍生了後續地持續性治療、照護，及個人健康記錄等長期的健康照護模式。

世界衛生組織（World Health Organization, WHO）提倡醫療機構對於患者的照護，應由以往較被動式轉變為主動預防式，也就是希望患者本身積極的參與醫療照護的部分。在這樣情況下，「個人健康紀錄」(PHR)[2]即為一個可行的解決方式，因為 PHR 能夠保存個人完整的醫療資訊，亦能透過病患本身的主動參與，由病患本身去維護個人的健康紀錄，並且可在之後與健康照護的提供者(醫師、照護者)進行有效的溝通[3]。由於所有就診過的醫療紀錄皆可透過網路傳送到 PHR 的伺服器上，患者可以查閱每次就診的資料，在醫療程序結束時將摘要等資訊提供給病患，能有效促進病患本身對自己照護的了解，改善病患與照護提供者的關係，增進病患照護的滿意度，且能激勵病患更願意投入未來健康照護計劃[4]。為了能和健康照護服務提供者進行良好的溝通，個人健康紀錄(PHR)就扮演了重要的角色，其除了能夠完整紀錄與保存個人的醫療資訊，更重要的是 PHR 是由患者本身去主動參與及維護[5]。因為所有接受過的醫療紀錄都會透過網路環境傳輸到 PHR 後端伺服器，而患者在通過認證後可以隨時隨地的存取每個醫療服務的資料，根據過往的研究，在每一個診療階段結束後可以適時地提供醫療摘要給患者，進而

促使患者們對自己健康照護上的了解程度，增加後續健康照護計畫的溝通能力，有效提升整體醫療服務的滿意度以及激勵患者更有意願的投入未來的健康計劃。

一個完整的個人健康紀錄(PHR)系統應具備幾項特點:使用者個人能夠管理自己的 PHR，並可以授權其 PHR 的權限之開放程度，亦即可以自己決定誰可以去存取，在哪裡存取，或是什麼時間才可以存取等多項權限。因為 PHR 系統記錄著患者們的全部醫療及個人資訊，甚至是健康照護提供者的資料，加上 PHR 系統存取的時間、地點都是較不限制的，因此必須確保在存取 PHR 系統上的資訊時是同時具備隱私性與安全性的。個人健康紀錄(PHR)不僅能提供給家庭醫師、主治醫師、專業護理人員、以及相關照護人員快速且更深入地了解患者本身的健康情形，做為後續作業上之參考，並可以在實踐居家照護(Home-Care)以及遠端醫療(Tele-health)上做為參考之依據;甚至，在未來能經過授權提供給醫療研究單位作為研究分析之用。而對於 PHR 系統的記錄內容目前並沒有一套非常完善且統一的標準介面，主要內容還是會依據患者所屬的醫療單位及照護型態，因此可能會根據治療或手術紀錄而有所改變。

資訊科技(IT)除了快速的發展外，還將許多科技整合在一起，例如奈米、感測、及生物科技等，進而衍生出新的概念或是新的資訊服務。這些新的資訊服務在許多產業中都能帶來新的突破。近年來，物聯網在高度的發展下，紛紛結合了 RFID、NFC 標籤或者是其他更微小的感測裝置整合成感測網路，未來將可以透過無線信號的網路環境建置各種產業中專屬的感測網絡環境，提升各種產業的競爭力，包括醫療產業也可以使用行動裝置與行動數據的環境。學者 Sitting 認為 PHR 可以結合各種網路服務模式，包含結合物聯網感測環境，以及安全健康照護系統等，並可提供使用的患者去維護自身的健康狀況，以及後續的醫療問題，藥物問題、或是照護諮詢等，並讓健康照護提供者與患者之間能有效的溝通與配合。而另一位學者 Markle Foundation 則表示 PHR 為一種多個網路工具的整合[6]，能讓使用者存取及整合自己終身的健康資訊，且讓有需要這些健康資訊的服務單位能取得適當且重要相關的資訊。然而由於無線信號有存在的弱點與風險，因此在無線的網路環境下，那些未經許可認證的使用者能夠更輕易地非法存取醫院的網路服務及資源。這些都可能包含許多安全性的問題。另外因為無線感測網路的資源有限，其標籤的記憶體小、運算能力低等問題，因此更多的威脅、攻擊、或漏洞都圍繞著無線網路環境。本論文將針對以物聯網為基礎的個人健康紀錄系統，探討

其身分認證與資訊安全議題。

## 第二節 研究動機

未來以患者為中心的個人健康紀錄管理架構可以讓使用者有足夠的權力去管理與維護自身的所有健康紀錄，例如:新增、刪除、修改等動作。此外將PHR系統建置在物聯網的多元感測網路環境下，能結合多種感測裝置，例如:血壓、心跳、體溫等測量器，不僅能透過感測器即時監控患者本身的身理訊息，亦能做長期生理資訊的收集，將所有收集的訊息透過網路媒介傳輸到後端伺服器或雲端上做整合管理,尤其是以結合雲端服務為主,使用雲端服務商提供基礎設施即服務(IaaS)、平台即服務(PaaS)和軟體即服務(SaaS)，除了能快速地存取並能有效的共享相關資訊，甚至於大幅降低醫療院所建置數據庫的能本，將更多資源往醫療研究的發展以提高醫療品質。

目前較常見的PHR服務系統，美國健康資訊管理協會(American Health Information Management Association, AHIMA)所提供的服務MyPHR,這是一個在無線網路環境下結合可攜式裝置的系統，提供給使用者將個人健康紀錄存放到智慧卡(Smart-card)、PDA、智慧型手機、以及隨身硬碟上與各個電腦設備進行資料交換的服務；也有結合網路服務的PHR系統，讓使用者能透過網路作業進行自我的健康資訊管理(例如:AHIMA, e-HIM Personal Health Record Work Group)[7]。此外雲端服務非常成熟的兩間提供商,Google和Microsoft也曾在他們的雲服務上開發相關的個人健康紀錄系統,分別是Google Health[8]和Microsoft HealthVault[9]。以Google公司在2008年推出的「Google Health」健康紀錄服務為例，美國各地區的Google Health使用者可以透過雲端服務紀錄本身的健康紀錄，而且這項服務還有延伸至各大藥局或診所，使用者、藥劑師、或是如醫師或其他醫療人員可以透過網路快速的存取這些紀錄。雖然這項產品於2011年因為某些問題而停止其服務，但仍可以看出像Google這樣的雲端服務商也積極地想朝個人健康系統發展。

基於物聯網架構建置的個人健康紀錄系統(PHR)服務是希望透過即時與長期的紀錄來改善疾病管理或是加強個人對本身的健康管理，除了即時的治療，也期望透過長期的紀錄來預防未來患病的可能並改善健康的方針，然而在使用更便利系統的同時，使用者也格外關注PHR或是其他醫療系統的安全性、隱私性、保密性等，尤其是建置在感測環境或是物聯網環境下，訊息的傳遞過程更為發散，比

起傳統的線路更容易被不法人士竊取身分或是在傳遞過程便將資料攔截進而偷取患者本身的醫療紀錄、醫療機構、以及照護人員等相關資料。於1996年健康保險流通與責任法案(Health Insurance Portability and Accountability Act, HIPAA)[10]中概述了醫療相關系統，包括PHR在內的隱私與安全之法律保護。

因此，在考量建置在雲端環境或是物聯網環境的安全機制是否能有效的保證其機密性和適當的存取權限仍是PHR必須要加強的環節。為了應對PHR系統在無線感測網路中曝露的風險與弱點或是在後端及雲端伺服器存取時可能面臨的風險，PHR系統提供者除了要靠密碼加密患者的資訊以及確保在傳輸交換過程不會有洩漏的可能，更重要的是個人健康紀錄系統應該要給予使用者，即是紀錄的擁有者完全的權限去控管本身的紀錄或是要開放的紀錄及要分享的對象。

儲存在後端伺服器或雲端服務上的患者個人健康資訊必須確保有足夠的加密系統能保護資料的機密性與隱私性，此外也必須保證使用者的資料在傳輸的過程中不會被截取，就算被竊取也能透過強大的保密機制而不會被破解，因此在無線感測的物聯網環境下導入PHR系統必須要更謹慎的評估其隱私和系統安全的保護能力，須有強健的身分認證技術以及加密演算法來完整保護使與者的隱私資訊。個人健康紀錄系統雖然有別於以往的紙張病歷，提供更便利的紀錄追蹤或是加密保護等，但如果是將其系統建置在物聯網的環境下，讓使用者端需要透過連上後端伺服器作存取動作，如果後端環境中沒有嚴謹的方法去認證使用者身分，則可能產生於過程中洩漏個人資訊的風險、濫用資料進行非法的行為、共享資源所產生的問題、以及資料或服務被竊取等問題，而這些威脅在HIPAA的法規中也尚未有完善的法律限制。因此，將PHR系統建置在物聯網的環境中，必須將所有紀錄經過完善的加密技術，產生密文後才能儲存與傳送，以防被有心人士侵入系統進而竊取或竄改使用者的隱私資訊。考量到物聯網中建置PHR系統所帶來的效益以及其所可能帶來的風險與威脅，本論文將提出一個完善的身分認證技術以適用於物聯網環境中的個人健康紀錄系統。

## 第三節 研究目的

因為網際網路的快速發展，在網上的交易或資料的交換越來越多，其途徑從私有網域到公眾的網路之間傳輸，媒介更是從有線逐漸轉變成無線網路的架構，隨之而來的是更多的安全問題需要被重視。未來的醫療環境會轉型成由無線感測

單元組成的物聯網環境，將以患者的自主管理意識為重心的PHR架構將建構在物聯網的環境中，其優點為有效降低管理成本、患者的資訊有效交換與分享、資源容易延伸至其他平台環境等優點，然而如果這些系統無法提供具備足夠安全性的身分認證與資訊傳輸機制的話，將得不到使用者的信任而可能導致系統無法有效的推行或是運作；另外一方面，物聯網的環境所面臨到的安全性與隱私性也一直是人們所重視的議題，因為物聯網中的感測節點繁多、資料傳輸的方向過於發散等，要如何確保使用者在使用時不會洩漏個人重要資料或是身分被不正當的認證且資料在傳輸過程中能同時達到便利性與隱私性的目標，也是非常重要的研究領域[11]。因此為了解決上述PHR系統可能產生的問題，必須有別於傳統加密技術的認證方式，設計一個兼具隱私性與安全性的加密機制並且適用應用在物聯網的環境架構。

建置在物聯網環境的個人健康紀錄系統須確保使用者的隱私資料在記錄過程與傳輸方式是具有足夠的安全性與隱私性的，而建立在這樣的原則下，PHR系統能有效的提升醫療品質、保障病患的隱私資料、同時能即時與長期地掌握患者的健康狀態。PHR系統應允許多位經授權許可的使用者(患者、家屬、醫療人員等)存取後端資料，為了確保PHR在傳輸與身分認證過程中不會被惡意人士攻擊、竊取、或竄改等情況，基於以上目的，本研究提出一個以雙線性配對(Bilinear Pairing)為基礎的密碼技術[12]，雙線性配對是利用線性映射函數(Bilinear Map)，藉由使用一個循環群(Group)對應到另一個循環群之間的映射關係，而使用其為基礎的加解密機制之安全性是建構在嘗試解開特殊問題之假設的困難度上，本研究中的架構亦結合了智慧卡(Smart Card)做安全的身分認證機制之環節，並加入時間因子做為時效性檢驗，確保只能在特定的時間內做存取動作，大大加強了其安全機制。

經授權的使用者藉由本文所提出的安全機制與後端系統連結與溝通，來做相關作業，如新增、修改、刪除等，在取得欲取得的資料時，並同時保障使用端與伺服器端之間途徑的安全性與隱私性，並經由後續的安全性分析，說明本論文中的方法能達到有效的安全之目的。

# 第二章 文獻探討

## 第一節 物聯網(Internet Of Thing, IOT)

物聯網(IOT)這個詞並不是代表一個全新的科技，它其實是將許多已經發展純熟的科技做一個應用上的整合，例如:各種感測裝置(體溫、濕度、溫度)、IPv6、無線網路的基礎建設等。而IOT的目的則是將生活中各式各樣的設備或物件串聯起來，賦予物件連上網的功能或是嵌入感測單元，例如:RFID Tag、環境感測器、生理感測器、GPS等，並透過網際網路將所有嵌入感測裝置連結在一起，形成一個大型的網路結構並與後端的伺服器或雲端系統串聯起來，使"物"與"物"之間能夠將感測到的資訊互相交換，達到自動對話的能力，並能夠智能的將接收到的訊息做適當的處理或回應，達到更便利、更易於管理的生活環境，亦能有效改善生活細節的掌控，實現真正的"智慧生活"。

### 壹、物聯網的架構:

物聯網(IOT)的標準架構共分為三個階層，依序為最低的感知層、中間的網路層、以及最高的應用層。以下為物聯網的架構圖。

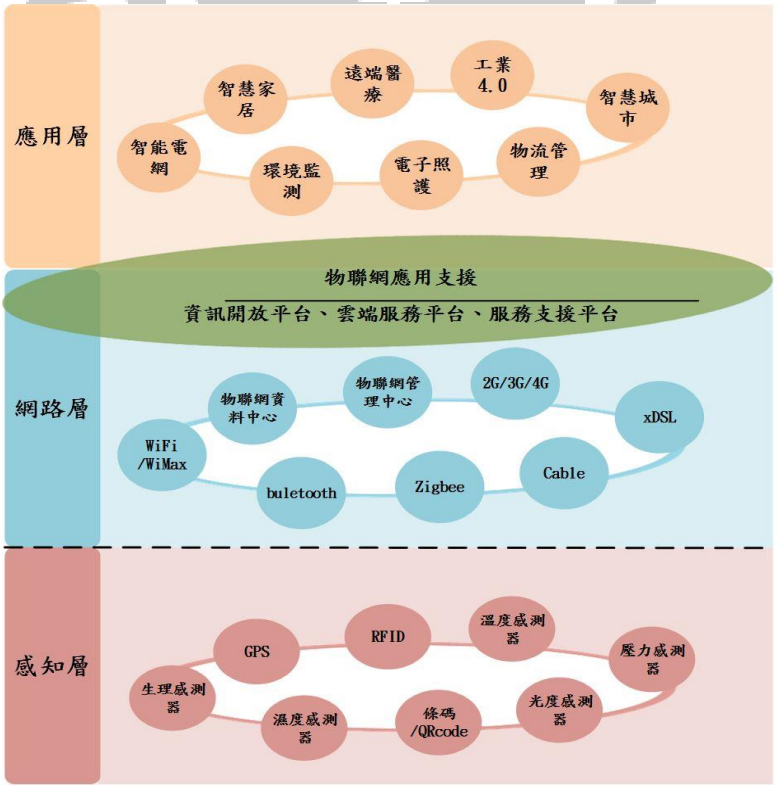


圖 2-1、物聯網架構圖

一、感知層

主要角色亦即物聯網裡稱的”物”，可由感測技術與辨識技術來組成，感測技術可以做為監控環境地理或生理的狀況，ex.壓力感測器、溫度感測器、速度感測器或心跳、脈搏感測器等；辨識技術用來遠端辨識或存取”物”的身分及資訊，常見的辨識裝置有 RFID、二維條碼、QRcode、iBeacon 等，因此將其結合並發展成感測網路。

二、網路層

網路層的主要工作是要處理由感知層傳輸上來的訊息，透過有線(RS232、Cable)或無線(3G、4G、Bluetooth、ZigBee)等媒介傳輸訊訊息，必須賦予每個”物件”相對應的 IP 位址來連上網路，且須確保能提供一個可靠、穩定的網路傳輸環境，其關鍵為 IPv6 隨時都能支援，因為需要非常大量的位址才能使物聯網有效運作，而 IPv6 的定址技術能提供足夠的位址。

三、應用層

為使用者實際接觸到各種 IOT 服務提供的階層，可因應企業或使用者各種不同的需求來建置其應用的服務或系統。使用者可以從任何時間、地點取得服務，並能連結後端伺服器或是雲端服務平台(SaaS/Paas/Iaas)，透過各種分析技術(ex.雲端運算、資料探勘、BI 等)分析感測裝置蒐集來的資料並將其整合成新的資源，以建構一個服務平台，提供符合需求的各種服務模式，常見的應用層應用有智能電網(Smart-grid)、智慧城市(Smart-city)、智慧居家(Smart-home)、電子照護(e-Health)、工業 4.0 等，從企業、政府、醫療、教育學習、工業、農業及居家生活等，都能建置在物聯網的環境中。

## 貳、物聯網的核心技術:

物聯網架構的實踐必須建立在三項技術的核心基底下，分別為無線射頻辨識技術(RFID)、感測網路、與M2M (Machine to Machine)，以下將依序說明:

一、RFID

無線感測射頻技術主要是運用在物聯網的感知層之中[13]，必須將物件嵌入 RFID 標籤，每個標籤都擁有唯一識別的電子編碼(EPC)，使物聯網中的物件都可以在讀取器的感測範圍內達到辨識，即使在移動過程中仍然可以做到。在整個物聯網網絡中將能互相分享與交換彼此的資訊，做到物件的追蹤、追溯或是

對環境的監控、以及各種資產的管理等，達到物件間的訊息相互交換與共用。

依據 RFID 在物聯網的發展架構下，用以下例子來說明:未來的乘坐工具-智慧汽車，在汽車上的各個零組件與引擎上加裝嵌有 RFID 標籤的感測器，若駕駛者在駕乘過程中汽車有異狀，即可自動感測到發生故障的零件或原因，給予駕駛者安全的警示，並將訊息傳送至遠端的伺服器中，讓維修人員可事先安排維修程序，亦因為已經感測到是哪個零組件出現問題，因此可以節省大量的檢查時間，馬上就可以對問題點進行處理，將可以大大的減少維護的時間。物聯網中的作業結合了各種應用，而 RFID 技術在這其中扮演了重要的感測與辨識的角色。以下是幾個 RFID 在 IOT 的應用實例:

(一) RFID 可以與溫度感測器結合，並將感測到的資料做為自動啟動空調的服務，延伸至物聯網的應用，可以透過 GPS 定位屋主的位置，並自動去計算屋主到家的時間去啟動空調和自動調整到最適當的溫度，讓屋主回到家中即可享受到舒適的溫度與環境並可達到節約能源的效果。

(二) 倉儲管理上可同時使用主動式與被動式 RFID Tag 以提升管理效能，先將貨品嵌入被動式 RFID Tag，而在搬運設備或運送貨品的載具嵌入主動式 RFID Tag，可由 Reader 讀取物件上 Tag 的資訊並整合起來後透過無線網路環境將整合好的資訊傳給載具上的 Tag，並可由後端伺服器即時從主動式 Tag 收到載具上貨品的資訊、數量及位置等訊息，因此可以降低盤點成本、出貨錯誤率，大幅提升倉儲管理效能。

(三) 智慧電子票卡的應用，將遊樂場或展覽場的入場票電子化，並嵌入 RFID Tag，可透過各場館的 Reader 快速的記錄入場參觀的遊客資訊並定位遊客所在位置，可以引導遊客參觀園區，以及各場館的人數監控。

## 二、感測網路

感測技術是將各種感應器(ex.溫度、壓力、速度)、全球定位系統(GPS)、掃描器(ex.影像、聲音)等感測裝置與網際網路，有線或無線的網路架構整合起來而形成的一個巨大網絡,讓所有具有 IP 位址與連上網能力的設備能和這一個巨大網路串聯在一起，即可快速地感測、辨識並與遠端的伺服器、人或其他物件做溝通，以提供管理或服務。例如，我們對某一種物件所能感受到的特徵、感官、或即時的變化之狀態等訊息，如果透過多種感測器感測或辨識裝置整合出

此物件的資訊並傳至網際網路上，在遠端的使用者或是其他裝置就能利用這些訊息來感受到這個物件的特性，甚至能夠遠端操作、遙控這些物件。

三、M2M

物聯網的目的就是希望能打造一個 M2M 的網絡，亦即機器與機器之間能夠對話的能力，而這邊所提到的機器可以是小到像一個塵埃的微型機器，也以大到像火車、太空梭等物體。而 M2M 也可以以一對一、或一對多的形式來溝通。將所有終端設備連接到一個雲端運算中心進行訊息的交換。M2M 不僅是機器與機器之間訊息的傳遞，而是機器與機器之間的能夠智能化、交互式的溝通，表示就算沒有通過人所發出的訊息，機器間也會透過接收到彼此間或感測到的資訊，智能的做判斷與處裡，感覺就是讓 "物"多了思想與智慧。其實不只是機器對機器，也有人認為是 Machine to Man 或是 Man to Machine，簡之物聯網是透過通訊技術來交換訊息達到人、機器、系統之間彼此的溝通。

參、物聯網發展的問題與挑戰:

物聯網(IOT)雖然近幾年有了快速的發展，但仍無法完全普及與實踐，其中包含了許多因素,因為有一些困難點像是安全性及技術上的問題需要去克服與探討，以下將針對安全性的問題與發展上的限制作個別說明:

一、安全性問題:

(一) 需做連結的"物"太多，且不同性質的物件傳遞的訊息中深度、廣度、複雜度皆不平均，因此在傳遞訊息的過程中容易出現安全性的問題。

(二) 傳遞的內容中包含大量個人、企業、醫療資訊、工業技術甚至政府的機密資料，容易吸引有心人士竊取隱私資訊。

(三) 目前已知多種竊取資訊及惡意攻擊的手法，例如竊聽攻擊、重送攻擊等侵入伺服器設備的手法，亦常有有心人士在物聯網的通信網路中散播惡意程式碼，讓許多存取到的裝置或系統發生異常甚至癱瘓，以及最難抵擋的分散式阻斷攻擊(DDos)等。

(四) 現階段的許多感知裝置、辨識裝置，例如 RFID Tag，因其結構太簡單不夠健備，因此很容易被偽造、竄改其感測到的或是本身內存的資料。

二、物聯網發展上的挑戰:

(一) 技術標準的整合:物聯網目前在技術已經夠完整與健全,但是不同產業各自發展出來的物聯網之標準、協定、介面都不全然相同，會導致訊息交換或傳遞上有整合上的問題，”物”與”物”之間也會有溝通上的困難，因此要讓物聯網真正實踐，必須訂出統一的技術標準能跨越不同層級(感知、網路、應用)與介面。

(二) 基礎建設(Infrastructure)不夠完善:感知層及應用層的技術已經有一定成熟度了，例如各類型感測裝置、資料探勘、雲端運算等，但網路層所必須涵蓋的的範圍還無法達到實現物聯網的需求，因為訊息的傳遞及交換的速度不夠快速，這也成為物聯網不能完全實現的難點之一。

(三) 將”物”智能化的成本昂貴:物聯網中的物件不單單是只能連網的”連網物”而已，而是要賦予其遇到任何情況能自能反應的智慧，但因智能化改造的成本昂貴，只靠企業本身的能力有限，因此需要企業之間的聯盟或是與政府之間有相關的政策或計畫，打造創新的商業模式，例如:想要打造智能城市而建置所需的智能路燈時，應配合政府的都市建造計畫擬定相關的合約與計畫內容。

## 肆、RFID 在 IOT 的運作

使用移動式或定點式的 RFID 辨識器(Reader)將裝有 RFID 電子標籤(Tag)的物件的內部資訊或感測蒐集到的訊息進行辨識或存取[14],並透過無線或有線的網路環境進行訊息的傳遞與交換，然後將這些訊息以標準化的介面或方法存放在資料中心、管理中心、後端資料庫、或是雲端上，之後只要是想要使用這些資料的使用者(例如:製造商、供應商、客戶等)、應用程式、或系統只要有授權認證都可以根據需求使用雲端運算、資料探勘、BI 等分析技術從這些資料中分析出符合需求的資源，而這種模式運作下可以利用這些資源建置在物流管理、農林產業、工業 4.0、以及醫療機構、甚至軍事設備上。未來不論是物品、應用程式等所有軟硬體只要是建置在物聯網中都可以透過資料快速的蒐集、傳遞、交換、轉換等方法進行智能的反應與回饋，將轉移整個典範，打造”智慧地球”。下圖二為 RFID 技術應用在物聯網架構之示意圖。

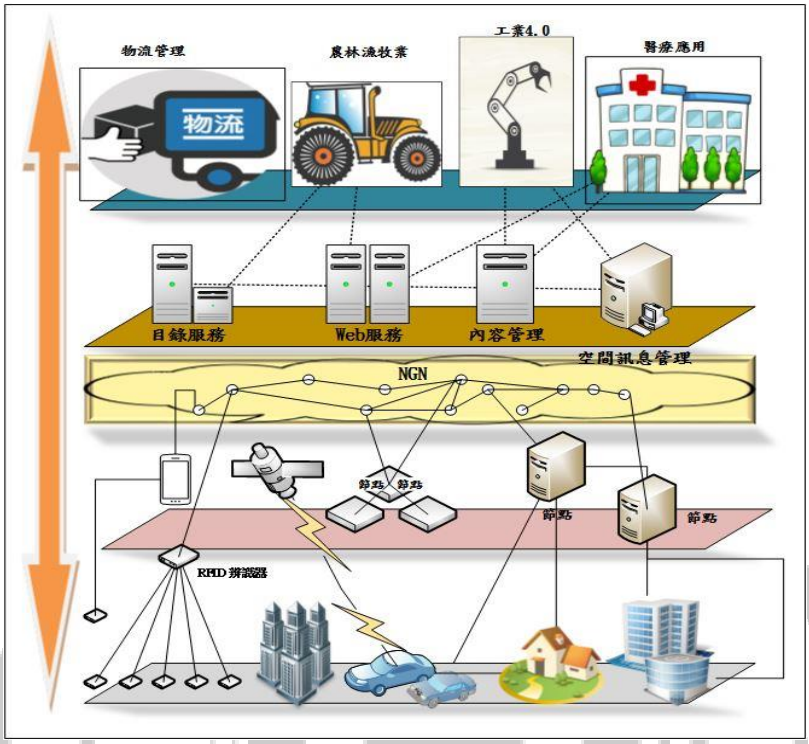


圖 2-2、RFID 應用物聯網之架構圖

## 第二節 雙線性配對(Bilinear Pairing)

學者Shmair於1984提出一個以身分認證為基礎(Identity-based Cryptosystem)的密碼系統[15]，其概念是希望利用使用者的個人資訊作為公開金鑰來作加解密，但由於缺乏一個有效率的加密系統，使得這樣的概念一直無法實現，直到學者Boneh和Franklin[16]以Weil pairing為配對方式的基礎之研究提出後，使得Weil pairing漸漸成為建構身分認證或是數位簽章的加解密工具。

Weil pairing可以將橢圓曲線上的點之集合映射到一個有限區域的乘法循環群上，藉此方法可將橢圓曲線上離散對數問題轉換成一般離散對數。因此Weil pairing之所以能扮演重要的角色，是因為其擁有雙線性配對函數的特性。而雙線性配對是利用兩個循環群(Cyclic Group)相互對應到一個線性映射函數(Bilinear Map)的關係，利用雙線性配對應用在橢圓曲線上所有的點之集合，皆能在代數幾何學上形成群的關係，在密碼幾何學的應用上，雙線性配對應有以下定義與特性，$G_1$為一個以序(Order)為一大質數q，生成元為p的群(Group)，而$G_2$也為一個以序為大質數q的群，其中$G_1$為一加法循環群，而$G_2$為一乘法循環群，則存在一線性映射函數 $\hat{e}:G_1\times G_1 \rightarrow G_2$。此配對的映射函式滿足以下三點:

1. 雙線性(Bilinear):

假定$P,Q,R$皆屬於$G_1$的點，則可以得到

$\hat{e}(P, Q+R)=\hat{e}(P, Q)\,\hat{e}(P, R)$,

$\hat{e}(P+Q, R)=\hat{e}(P, R)\,\hat{e}(Q, R)$,

此外任何滿足$a, b\in Z_q^*$會成立如下公式，

$\hat{e}(aP, bQ) = \hat{e}(abP, Q) = \hat{e}(P, Q)^{ab}$

2. 不可退化性(Non-degenerate):

若存在$P$為$G_1$之生成元，則$\hat{e}(P, P)$也會是$G_2$的生成元，亦即$\hat{e}(P, P)\neq 1$

3. 可計算性(Computable):

如果$P,Q$皆屬於$G_1$的生成元，則$\hat{e}(P, Q)$能被有效率的計算出

本文中的安全可靠性是使用雙線性Diffie-Hellman問題的假定，簡稱BDH。利用BDH進行雙線性配對[17]，其問題是指定給$(P, aP, bP, cP)(a, b, c\in Z_q^*)$，若在不知道$a, b, c$的情況下，要計算出$W=\hat{e}(P, P)^{abc}\in G_2$是不可行的，其中$\hat{e}$是一映射函數: $\hat{e}: G_1\times G_1 \rightarrow G_2$，$P$是$G_1$的生成元，目前已知還沒有一種方法能有效地解決BDH的問題，因此可以認定雙線性配對的問題假設是一困難問題，並具有合理的安全性與機密性。

## 第三節 PHR 介紹

個人健康紀錄(PHR)為一個以個人的醫療與健康相關之所有紀錄之整合與應用，並將其數位電子化之應用[18]。目前大多數醫療服務機構的醫療資訊系統皆依據HIPAA的規定以及採用HL7之七層架構，而PHR系統能以標準化的儲存格式符合各級醫療機構的資訊系統。它能紀錄關於使用者所有的生理狀況、用藥資訊、就診資訊、健檢結果等資訊[19]，並長期地去更新與保存。而依據美國衛生資訊管理協會(American Health Information Management Association, AHIMA)的定義，PHR的主要目的是記錄使用者的所有健康資訊，包含短、中、長期的醫療記錄，而這些記錄在使用者就診、用藥諮詢、甚至是未來的飲食保健計畫時都可以做為參考的依據。PHR亦是一個攜帶性高且具有較高的彈性與擴充性的紀錄資料，因此能夠延伸至不同層級的醫療機構或是地方藥局等，PHR系統可以整合從醫療院所的診斷結果並和使用者個人的日常生理健康記錄做結合，並做一個長期持續性的健

康紀錄，包含使用者的飲食狀況(三餐內容、卡路里、營養成分)、生理狀態(心跳、血壓、血糖)、運動行為(運動頻率、性質)，及其他相關的醫療紀錄，讓使用者能夠更清楚地去了解自己的身體狀況，除此之外亦能提供給醫學上之研究[20]。PHR系統應具有以下特性[21]:

一、使用者可以擁有絕對的權力去支配自己的PHR，並能決定哪些部分可以開放給認證的人去存取，以及設定其時效性等狀態。

二、PHR應涵蓋使用者生平所有的醫療紀錄與其他健康照護資訊。

三、PHR可以打破時空的限制，在任何時間與地點都可以存取。

四、PHR系統在存取與傳輸過程必須具備隱私性與安全性。

五、PHR的擁有者可以清楚地檢視到其紀錄什麼時間點被存取以及所做的新增或修改等。

六、PHR能讓醫護人員作為在醫療機構中的個人病歷之擴充，反之亦可允許醫療機構中的個人病歷紀錄放置在PHR系統中，增加其完整性。

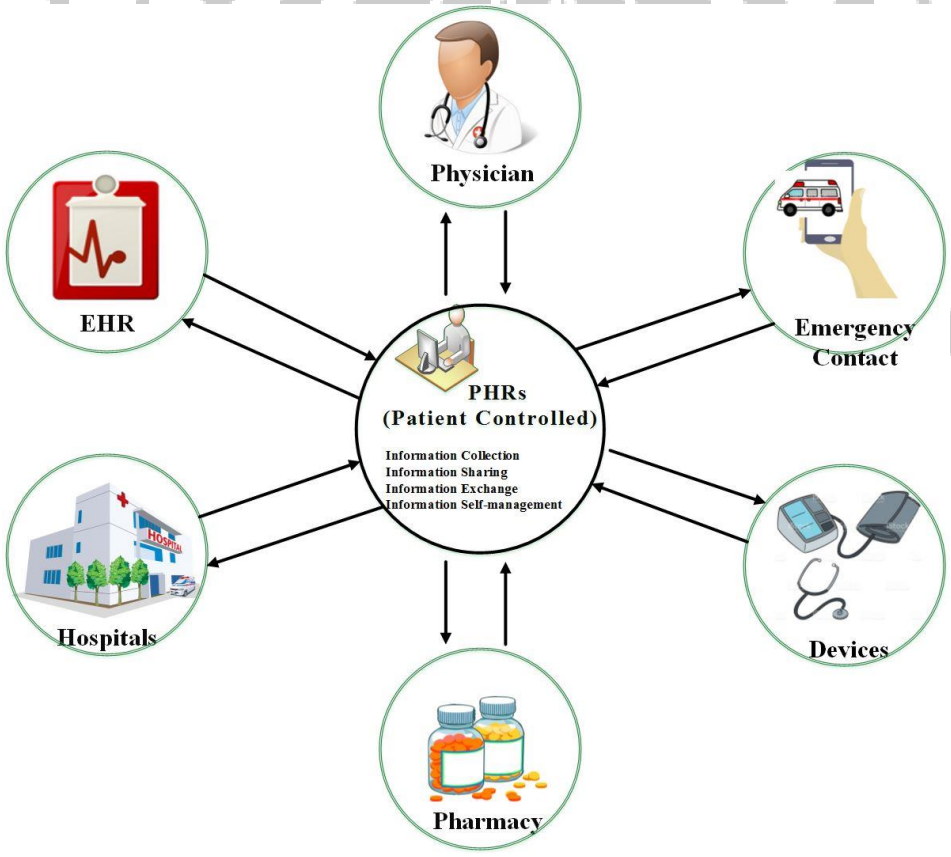


圖 2-3、PHR 系統架構圖

一個完整的PHR系統應具備以下幾項優點[21]:

一、使用者可以藉由使用個人健康紀錄來觸及更多的健康資訊，以達到自主地自我健康管理，有效改善個人的健康。

二、PHR系統能有效建立使用者與醫療照護服務提供者之間的橋樑，加強彼此之間的溝通能力。

三、增加醫療照護人員對患者生理健康狀況的掌握度，除了能提供即時的醫療照護，也有助於規劃未來的健康計劃。

於2009年，美國提出的經濟與臨床健康資訊科技法案(The Health Information Technology for Economic and Clinical Health Act, HITECH)大大的改善了過往使用的健康保險之流通與責任法案(HIPAA)對醫療資訊所訂定的隱私與安全之相關保護規範。

個人健康紀錄系統可以收集來自多種來源的患者健康資料，包含患者藉由自動感測裝置或是手動量測的生理狀態紀錄(例如:血壓、心跳、血糖等)、或是醫師的看診紀錄(例如:病例、醫囑、用藥處方等)、健康檢查紀錄(如:心電圖、X光片等醫療影像)、以及其他相關文件，如法律文件、委託書、保險文件等，此外PHR也能其他醫學相關的知識建置在系統上供給使用者需要時的參照標準，例如:緊急醫療處置、用藥相關諮詢資料、甚至是其他非醫療的保健管理知識等。

雖然PHR系統有部分資料可能來自於電子病歷紀錄(EMR)系統中的資料庫，但有別於EMR這樣的嚴謹，PHR的紀錄沒有嚴格的完整性(Integrity)和不可否認性（Non-repudiation）之要求。然而PHR必須建置在安全且隱私的環境下才能存取，並且需要足夠的權限才能讀取或修改文內容，很重要的一點是PHR的紀錄並不會取代其他合法紀錄的內容，例如:健保資訊。PHR是患者與醫療照護人員之間溝通的通道，除了有清楚地描述關於患者的基本資料與生理資訊，也有其所接收的醫療之紀錄，適用於即時的醫療服務以及規劃未來長期的醫療照護計畫。

若個人健康紀錄能有效的成為與醫療照護人員溝通的管道，則能藉此節省相關成本，溝通所需的時間等；個人健康紀錄也能結合個人與其有關聯的對象，例如:父母親與孩子或其他親屬之間的健康紀錄等，並由使用者主動地去維護與管理，或是藉由其他感測設備去自動更新等，PHR的推動將能大幅提升醫療服務品質，因此個人健康紀錄的推廣將有其實用與必要性。PHR系統也能增加健康維持的提醒功能；幫助患者改善與醫師之間診療過程的溝通與互動能力，並能即時的得到健檢的結果報告，個人健康紀錄系統還能提供用藥提醒功能，協助使用者辨識較

模糊且可能出現誤差的程序與服務。個人健康紀錄可以提供給使用者即時的照護計畫，並能隨時更新其計畫，以改善並提升照護的品質，PHR將提供持續、全面的照護模式，並能更有效率的成為患者與相關醫療人員之間最好的溝通工具，亦可化簡不必要的檢測程序與減少不必要的服務資源，節省許多成本。此外，透過嚴格的身分驗證與安全控管,讓使用者在享受自主的管理與維護個人健康紀錄時，亦能無需擔心私密資料的安全性與隱私性，使得在分享個人健康資訊時能有更多選擇性。更重要的是個人健康紀錄能降低醫療成本,簡化複雜且重複的醫療程序，更快速的回覆患者需求，並減少誤診的機率與風險，因此PHR系統確實能帶來更大的效益。

除了考量到個人健康紀錄的安全性外，PHR系統的架構應基於必須完整將使用者的的紀錄存放在中央伺服器，以及確保每個患者都能保有對本身的記錄全部之權利。以上，一個完整的個人健康紀錄系統我們必須考慮到以下幾個要點：

一、整合有關患者一生的完整健康醫療資訊；並能結合多重來源端的醫療資訊，不只是單一的醫療服務提供者的醫療相關紀錄。

二、必須提供一個穩固且安全的資料儲存端；並能透過網際網路隨時隨地存取後端資料庫，無時空限制的方便管理及存取。

三、使用者能確保保有完整存取 PHR 的權利；以患者為中心的個人健康紀錄系統，使用者可以決定能存取的對象以及移除過期的權限。

四、能準確地設置不同使用者對患者 PHR 的存取權限;醫生只能存取自己診療服務範圍的病患，如果病患轉診到其他科別，那麼新的存取權限必須能正確且即時的移轉給新主治醫師。

五、必須提供兼具安全性與隱私性，並能長期持續的完善健康管理機制。

未來個人健康紀錄(PHR)可以結合居家照護(Home-care)與遠距醫療服務(Tele-health)[22]，也能提供為醫學研究所需之樣本，因此當PHR服務的範圍不斷的擴充時，正確的授權給與適當使用者之行為成為了非常重要的課題，因為個人健康紀錄中的資訊是極具個人隱私的資料,需要完全經由使與者去決定其授權範圍，包含受授權的對象、授權時效性等等，以確保資訊的安全。因此PHR系統不僅需要保護後端資料之安全性外，亦必須做好嚴格的身分驗證機制，最後也要保證資訊再傳輸的過程中具有足夠的安全性，尤其是運作在物聯網環境下的個人健康紀錄系統，更需要保證個人隱私以及傳輸之安全隱私性。

# 第三章 研究方法

隨著近年來不斷推行個人健康紀錄等相關計畫，提倡由患者為中心的自主維護與管理自身的健康狀況與照護計畫，亦有越來越多的醫療院所參與 PHR，不僅能加強患者與醫療照護人員之間的溝通，還能有效降低成本，增加營運效能等。加上近來物聯網與無線感測技術不斷的完善，醫療業者結合這些技術並開發了許多穿戴式感測裝置，例如:體溫、心跳、血壓等，將能夠更快速且精準的紀錄個人的健康狀況，以及透過無線網路的環境傳輸資料到後端伺服器，並整合運用這些資訊。

在物聯網的環境中，PHR 系統運用在健康照護上，能帶許多優勢，並增加使用者主動參與醫療計畫之意願，但因為 PHRs 系統紀錄的資訊廣泛，像是就診紀錄、用藥紀錄、生理資訊等，使用上可能為多重使用者，患者本人、主治醫師、家屬、照護人員等，且延伸的平台也有許多，像是居家、醫院、甚至是當地的藥局，因此需要得到授權的角色、地點繁多，因此在 PHR 系統上的動態存取機制必須要相當完善，能確保使用者在存取資料時能得到身分的驗證，以及資料在傳輸的過程中，也須確保其隱私性和安全性，因此本研究以上述的種種安全性為考量，將提出一個有效的身分認證機制來驗證是否為合法的使用者。

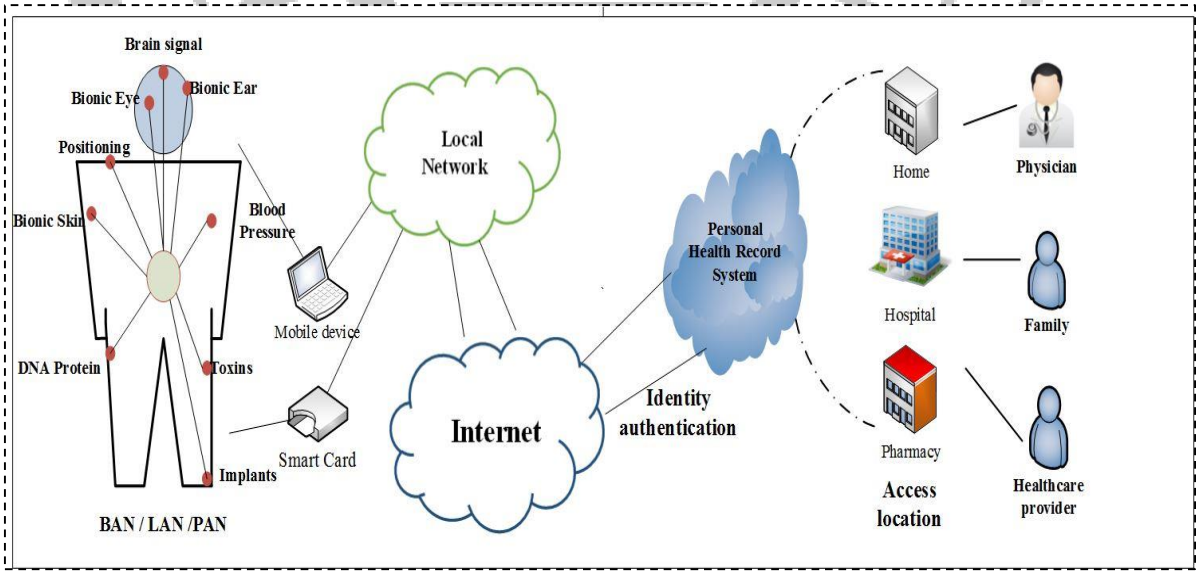


圖 3-1、PHR 系統架構

## 第一節 驗證機制與架構

利用感測裝置與物聯網架構將蒐集到的資訊傳輸至後端PHR系統，並讓合法使用者能夠隨時隨地的去存取資料是存在相當高的風險，個人生理資訊是屬於非常隱私的資料，並且同一個PHR的合法使用者可能有多位，且較開放式的網路環境相對存在較多洩漏的風險，為了改善個人健康紀錄所存在的風險，以及適用於物聯網架構之因素，本研究將提出一個完整的身分認證機制。

此機制將結合後端的信任資訊管理中心(TMIS)伺服器，所有存在的使用者(患者本人與經授權的人員)，若需要存取到PHR裡的資料，則必須先向TMIS申請，經申請通過，TMIS會交給使用者一張智慧卡(Smart Card)，以後使用者在登錄系統時必須配合智慧卡才能得到認證，綜合上述，完整的使用者的身分認證系統可分成三個階段:註冊階段、登錄階段與驗證階段，如下說明：

一、 註冊階段：使用者須先跟管理者或認證中心提出申請，經過審核後，管理者會給予使用者身分認證的資料，例如:智慧卡或通行密碼等，此時使用者才具有存取系統資訊的權限。

二、 登錄階段：當使用者要登錄系統時，須出示管理者給予的身分識別資料，用來驗證身分。

三、 驗證階段：管理者會依照使用者所出示的資料，例如:帳號、密碼、智慧卡等，來驗證是否為合法的使用者，若是合法的使用者即可存取系統的資訊。

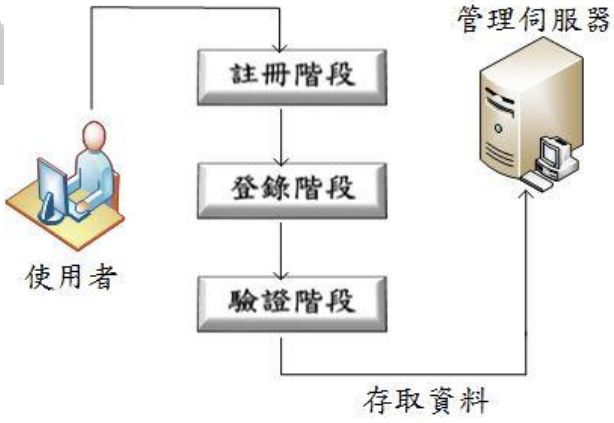


圖 3-2、身分認證流程圖

## 第二節 身分認證機制

醫療相關的照護系統或是PHR系統在任何情境下，都必須擁有完善的機制來保護使用者的隱私，這是非常重要的一環，例如:有些有特殊疾病的病患，並不想讓人知道。尤其當這樣的系統建置在以物聯網為基礎的架構下，多以感測裝置與無線網路作為資料蒐集與資訊傳遞的方法，這些因素與環境使得傳統網路的安全性架構和協定並不適用，因此本研究設計一個能在無線感測環境下的認證方式，藉由使用者所配戴的感測設備、行動裝置與基地台之間的安全傳輸協定與身分認證機制，確保使用者資訊安全性與隱私性能得到保護。此外在資料存取動作的環節也加入了時間參數，由此可限制得到授權並允許使用的人員在特定的時間內完成，並且能夠在規範時間內讀取資料，不需重複地驗證身分，以提高效率。本研究中完整的身分驗證機制將採用智慧卡(Smart Card)與通行碼的(Password)雙重身分認證，其驗證過程共有四個階段分別為初始階段、註冊階段、登錄階段、及驗證階段，以下將會個別說明:

表 3-1、參數與符號定義表

| 參數與符號 | 定義 |
|---|---|
| $G_1$ | 一個加法循環群(Additive Cyclic Group)，序(Order)為一個大質數 q，生成元為 $P_0$ |
| $G_2$ | 一個乘法循環群(Multiplicative Cyclic Group)，序亦為大質數 q |
| $H_1：\{0,1\}^*\rightarrow G_1$ | 一個單向雜湊表示式，輸入為$\{0,1\}^*$，輸出為 $G_1$ 中的元素 |
| $H_2：G_2\rightarrow\{0,1\}^*$ | 一個單向雜湊表示式，輸入為 $G_2$，輸出為$\{0,1\}^*$中的數值 |
| $\alpha,r,r'$ | 皆為由伺服器選擇的一個隨機值 |
| $Z^*_q$ | 整數數值的集合群 |
| $P_{pub}$ | 表示由伺服器所計算的一個公開金鑰 |

| | |
|---|---|
| $ID_u$ , $PW_u$ | 分別表示使用者註冊的帳號與設定的通行密碼 |
| $Q_u$ ， $D_u$ | 分別表示使用者的公開參數與私密參數 |
| $W$ | 由伺服器所計算的一個數值，並儲存在智慧卡中 |
| $\mathcal{V}_u$ | 由智慧卡計算出來的參數值 |
| $(a\|\|b)$ | 表示一個字串 a 與字串 b 所串接的連續字串 |
| $h(.)$ | 表示對()的參數集合字串做一個單向雜湊 |
| $T_{\text{Loin}}$ , $T_{\text{now}}$ | 表示系統登錄所花的時間以及現在的時間點 |
| 會議金鑰$(sk, sk')$ | 分別為伺服器端與使用者端所計算的會議金鑰 |

壹、初始階段:

Step 1: 信任資訊管理中心(TMIS)伺服器選擇一個線性映射函數(Bilinear Map) $\hat{e}: G_1 \times G_1 \rightarrow G_2$ and $P_0 \in G_1$。

Step 2: 伺服器生成兩個單向雜湊方程式(One Way Hash Functions) $H_1$與$H_2$。

$H_1: \{0,1\}^* \rightarrow G_1$

$H_2: G_2 \rightarrow \{0,1\}^*$

Step 3: TA伺服器選擇一個隨機數值$\alpha \in Z_q^*$，並且計算出一個公開金鑰$P_{pub} = \alpha * P_0$。

貳、註冊階段:

Step 1: 使用者向TMIS伺服器註冊一個合法身分的$ID_u$以及設置通行密碼$PW_u$。

Step 2: 使用者透過安全的通道傳送註冊請求給伺服器，內容包含$\{ID_u, PW_u\}$。

Step 3: 在收到註冊請求之後，伺服器會檢查使用者的合法性。

Step 4: 伺服器為使用者計算$Q_u = H_1(ID_u)$及$D_u = \alpha * Q_u$，其中$Q_u$是公開的參數而$D_u$是私密的參數。

Step 5: 伺服器選擇一個隨機數值$r$並計算參數$W = r * P_0$。

Step 6: 伺服器將個人化使用者專屬的智慧卡，卡中包含的參數內容有{$h(.)$, $ID_u$, $PW_u$, $D_u$, $\mathcal{W}$}， $h$表示一個由伺服器生成的單向雜湊方程式,並儲存在智慧卡中。

Step 7: 伺服器將智慧卡安全且私密地交給使用者。

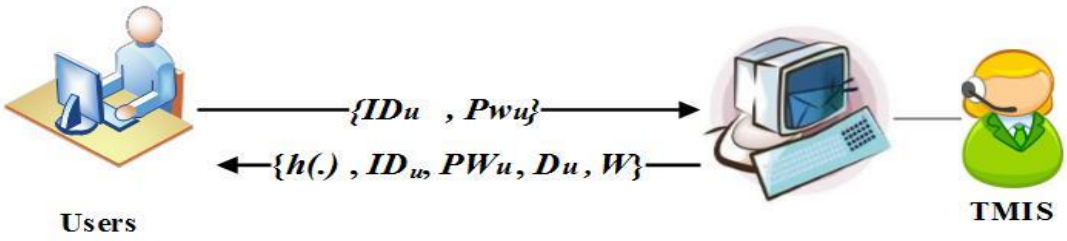


圖 3-3、註冊階段

參、登錄階段:

使用者將智慧卡插入裝置並輸入註冊時所設置的$ID_u$與通行密碼$PW_u$，之後智慧卡將會依序執行以下幾個步驟:

Step 1: 智慧卡會檢查使用者輸入的$ID_u$與通行密碼$PW_u$是否正確，比對儲存在智慧卡裡的資料是否與輸入的一致，若比對吻合，則執行步驟2。

Step 2: 智慧卡計算出$\mathcal{V}_u = D_u * \mathcal{W}$。

Step 3: 智慧卡傳送{$T_{Login}$, $ID_u$, $\mathcal{V}_u$}等資訊作為請求訊息到伺服器，$T_{Login}$表示登錄系統所花費的時間。

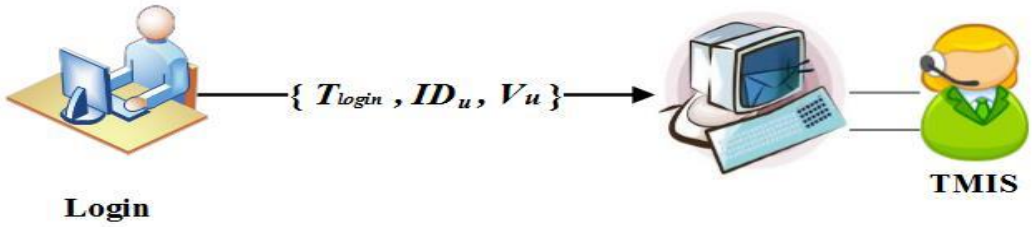


圖 3-4、登錄階段

肆、驗證階段:

伺服器從使用者端收到登錄請求與參數{$T_{Login}$, $ID_u$, $\mathcal{V}_u$}後，會透過以下協定驗證使用者身分:

Step 1: 伺服器會檢查$T_{now} - T_{Login} < \Delta T$是否成立，$T_{now}$表示系統目前的時間，而$\Delta T$則表示為傳輸延遲的時間。如果判斷成立，且$ID_u$被伺服器驗證為合法的，則

執行步驟2。

Step 2: 伺服器驗證$H_2(\acute{e}(P_0, \mathcal{V}_u))$是否等於$H_2(\acute{e}(P_{pub}, Q_u * \mathcal{W}))$，如果條件判斷式成立，則伺服器核准使用者的登錄請求。

Step 3: 於是，伺服器生成一個隨機數值$r'$且計算出一個會議金鑰$sk = h(D_u * P_0)$，以及 $h' = h(sk||r')$，並將參數$\{h', r', P_{pub}\}$傳給使用者。

Step 4: 使用者端計算$sk' = h(Q_u * P_{pub})$，並採用使用者的公開參數$Q_u$來驗證$h'$是否等於$h(sk'||r')$。如果條件成立，伺服器端即為正確的；如果不成立，則請求將會被使用者終止。

Step 5: 隨後使用者端計算出$h'' = h(sk'||ID_u)$，並傳送給伺服器端。

Step 6: 在收到$h''$之後,伺服器會驗證$h''$是否等於$h(sk||ID_u)$。如果條件式成立，則雙向的認證就完成了。使用者為真實且合法的，並可以被准許存取TMIS伺服器的資源。

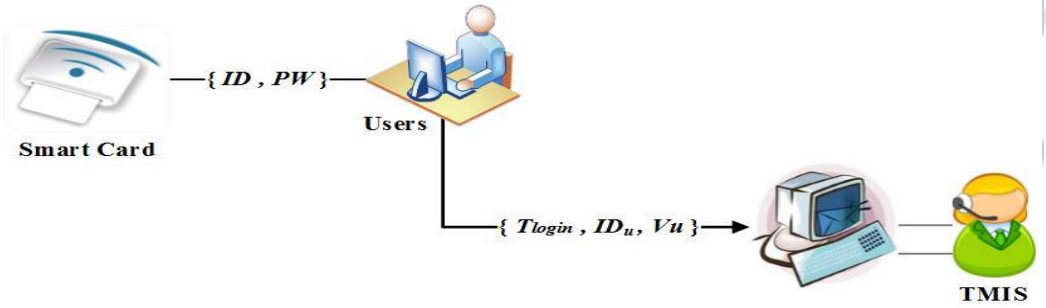


圖 3-5、驗證階段

## 第三節 應用情境

這個部分用來描述本論文中身份認證方法的應用與其應用情境，一開始會假定使用的情境；再來會描述整個驗證過程的細節，一個個人健康紀錄可能會將資料殂存在後端伺服器或是雲端上，並需要使用者本身去完全的管理，以及可能開放權限給其他多位使用者，醫師、家人、護士、照護人員等，每個角色都必須申請唯一帳號以及專屬的智慧卡，以及使用智慧卡才能登入系統中，並只有在完成驗證後才能存取與使用服務端的資料。

### 壹、情境一:

Step1: 假設現在有一位健康狀況分析師，須透過雲端存取患者的 PHRs 並檢視來評估其健康情形，並給予患者改善健康的建議。

Step2: 他/她必須先向信任資訊管理中心(TMIS)註冊一個合法的帳號 $ID_i$，並設定其密碼 $PW_i$，之後 TMIS 會計算出使用者的私鑰$D_u = \alpha * Q_u$，並個人化分析師的智慧卡一張，再交到他/她手中。

Step3: 登入系統時，先將專屬的智慧卡插入裝置中及讀取，之後鍵入自己設定的 $ID_i$ 與密碼 $PW_i$，系統會使用私鑰去計算$\mathcal{V}_u = D_u * \mathcal{W}$。並發出請求訊息$\{T_{Login}, ID_u, \mathcal{V}_u\}$給伺服器端，$T_{Login}$ 表示登錄時所花費的時間。

Step4: 伺服器端會計算並驗證$\acute{e}(P_0, \mathcal{V}_u)$是否等於$\acute{e}(P_{pub}, Q_u * \mathcal{W})$，等同才會接受使用的請求訊息。

Step5: 接受請求後，服務端與使用者端會相互計算出$h'$與$h''$，並傳送給對方作雙向的身分交互驗證之動作，只有當雙方都能完成驗證動作後，健康分析師才能存取服務端上的資源。

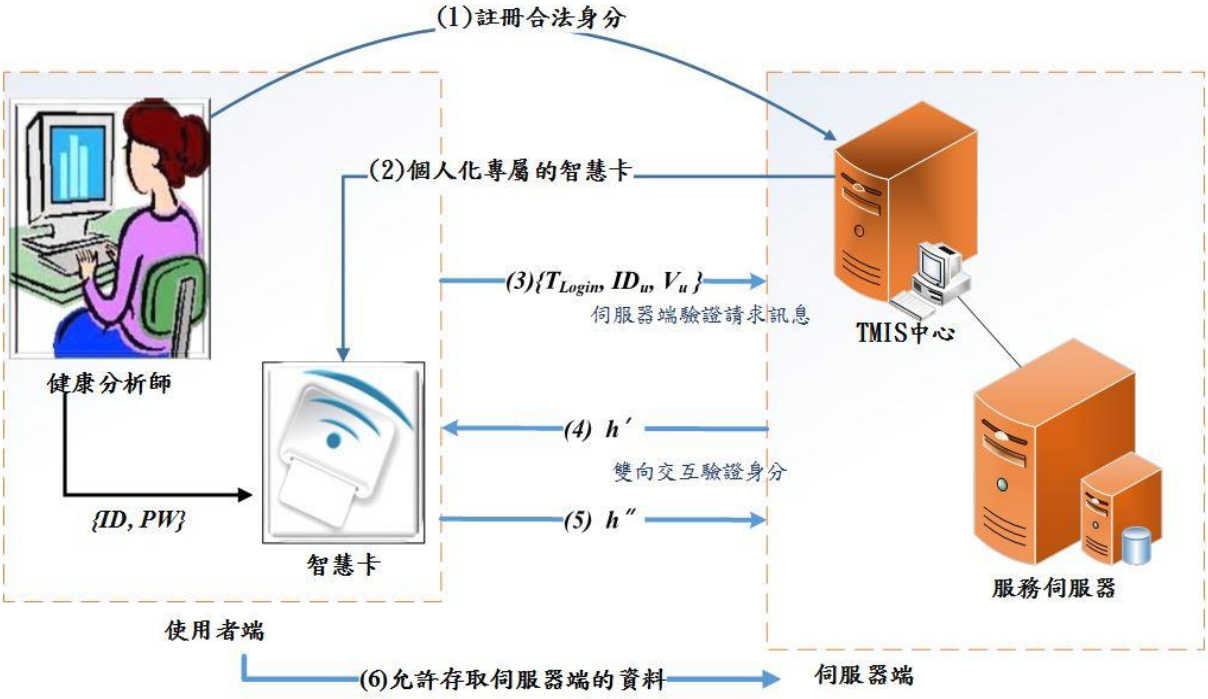


圖 3-6、應用情境說明圖

# 第四章 安全性分析

## 第一節 密碼保護機制(Password Protection)

一個建置在物聯網的個人健康紀錄系統，目的是透過使用者自主管理並結合其他醫療照護資源，進而改善使用者的健康狀況，因此其使用對象除了擁有者外，還可能包含經過授權的人例如:家屬、醫師、及相關照護人員。而每一位系統的使用者皆擁有個人的 ID 與設定的 Password，欲登入系統時必須鍵入設置的密碼才會准許進入，但在使用密碼登入的階段時，必須確保密碼不會被有心人士竊取並利用此來入侵系統，因此在對應的保護上所需求的可靠性與安全性是相對重要的，此外必須保證密碼具有不會外洩的風險，以及完善地保護機制，以下為幾種常見透過竊取使用者 ID 與 Password 登錄系統的的攻擊手法:

### 壹、竊取密碼驗證之攻擊:

這種類型的攻擊方法之目的是欲從伺服器端偷取用戶的驗證資料表，像是儲存在後端的ID與PW之雜奏值等，本論文的方法中，因為伺服器不需要儲存使用者的驗證表單，改將其儲存在智慧卡中，使用者也無法得知雜湊處理後的資訊為何，因此可以避免被竊取驗證表單這樣的攻擊手法。

### 貳、連線猜測密碼攻擊:

這樣的攻擊方式為連線到目標的主機，再透過密碼的猜測、追蹤等方法來登入目標帳戶，但是在登入的過程中，必須得到由智慧卡所計算出來的參數值$\mathcal{V}_u$，以及使用者的私密參數$D_u$，並破解$D_u$來取得使用者的密碼，由於此私密參數是使用雙線性映射(Bilinear Map)$\hat{e}$來演算加密的，因此有心人士想要破解必須解決雙線性的難問題假設才能破解參數，而這樣的攻擊方法在本論文中是非常難以實現的，加上必須在限制的時間內($T_{\text{now}} - T_{\text{Login}} < \Delta T$)破解才不會被伺服器拒絕存取，因此想要用連線密猜測破解是不可能的。

### 參、線下猜測密碼攻擊:

這種攻擊方式一般會透過攔截數據資料和其他漏洞來獲取目標用戶的密碼、或是有些會使用社交工程等手法來竊取帳密、也有透過特定軟體程式使用暴力破解法連續嘗試密碼組合直到得到正確結果。在本系統中即使攻擊者攔截到了由智

慧卡所計算出來的參數值$\mathcal{V}_u$，但攻擊者能仍然要解決難問題的假設才能破解私鑰$D_u$，此外攻擊者還必須解決單向的雜湊函式$H_1$和$H_2$，並猜測出由TMIS伺服器存在智慧卡中的參數$W$以獲取資訊，條件幾乎不可能實現，因此對於線下的密碼猜測的保護是安全的。

## 第二節 重送攻擊(Replay Attacks)

藉由中途攔截訊息並加以竄改並重送給目的地端的一種攻擊手法，在本文中這樣的攻擊方法幾乎不可能實現，系統端在收到登入請求後會去驗證時間間隔($T_{now} - T_{Login} < \Delta T$)在否在合理的延遲範圍內，若判斷不成立，則此 ID 會直接被認定為不合法的，因此拒絕登入系統之存取，透過攔截訊息和重送的方式在登入請求時會無法通過時間差的驗證，因此這樣的攻擊手法在本研究中是無法執行成功的。

## 第三節 偽造合法使用者攻擊(Impersonation Legal User Attack)

偽造合法使用者的攻擊方式是一種典型且最常見的方法之一，攻擊者藉由攔截到請求訊息之後，並可以使用該訊息來偽裝成合法使用者並登入系統存取資料。在本架構中，攻擊者的目的是要攔截由使用端傳送給伺服器端的請求參數{$T_{Login}$, $ID_u$, $\mathcal{V}_u$}。在本文提出的驗證方法中，使用者的登錄時間間距會被驗證，使得擷取到的請求訊息會因為時間逾時而請求無效並能防止有心人士登入系統。

此外攻擊者亦缺少合法使用者的密碼以及由 TMIS 伺服器存在智慧卡中的參數 $W$，使得攻擊者無法登入系統中，從攔截到登入請求訊息中破解使用者密碼或是從智慧卡中獲取都是非常困難的，因此難以偽造合法用戶的註冊訊息。想要破解使用者私鑰 $D_u$ 則必須先解決難問題的假設，或是只能靠竊取智慧卡以取得 $D_u$ 並破解。因此偽造攻擊的手法在本文中並不適用。

## 第四節 偽造合法服務提供者之攻擊(Impersonation Legal Server Attack)

這類型的攻擊方法是偽造合法的伺服器讓使用者誤以為是合法的，並利用使用者對攻擊者的信任，藉此竊取使用者的帳密或其他認證參數，以此順利登入爭正的服務端，或是當使用者上傳私密的健康隱私資料、就診紀錄、及其他資訊時，

就會被偽造的伺服器蒐集並一覽無遺。因此當攻擊端收到使用端的請求參數{$T_{\text{Login}}$, $ID_u$, $\mathcal{V}_u$}，即使攻擊方收到並來自使用者的請求訊息，但因為本文使用端與伺服器端必須以計算出的$h'$與$h''$作雙向驗證，而偽造端會因為缺少重要的的參數 $D_u$ 而無法計算出能被驗證$h'$，即使偽造端想從接收到的$\mathcal{V}_u$破解出 $D_u$ 也必須要知道存在智慧卡中參數 $W$ 的內容才有辦法，就算得知了 $D_u$ 也須克服雙線性中難問題的假設，因此無法成功作雙向驗證，想要偽造合法的伺服器端竊取使用者上傳的隱私資料，在本研究的認證中方法幾乎是不可能的。

# 第五章 結論

使用物聯網架構來建置的個人健康紀錄系統需要一個完整的身分安全機制來保護使用者的隱私紀錄，才能獲得使用者足夠的信任，並藉由 PHR 來改善個人健康的品質與未來健康規劃。由於物聯網環境下，往往是使用無線網路的架構，相較起來過於開放，而使用者必須將個人的健康隱私紀錄傳送至後端或是從後端存取之前的紀錄等，相對地傳統的身分安全機制與安全協定可能不適用在這樣的架構下。使用者在存取資料的期間，有效的身分認證技術可以保護用戶隱私資料的安全性與隱私性，因此身分認證機制是本論文中 PHR 系統應用上的關鍵因素。

透過安全且合法的認證系統能夠確保只有在經過身分驗證後的使用者才能登錄系統並存取系統資源。因此，在利用感測裝置結合物聯網架構建置的個人健康紀錄系統，必須提出可靠的身分認證機制。而當使用者在家中日常地記錄自身的健康生理狀況或是在醫院的就診醫療紀錄、以及用藥處方紀錄等，都可以透過系統持續且長期地記錄著這些資訊，並將其儲存在後端伺服器中。在日後，使用者及其家屬或是醫療照護機構的服務提供者可以遠端的查看這些健康紀錄，藉由觀察患者生理狀況的長期變化，達到預防與促進改善之目的，並可在日後就診時，讓醫療院所的醫師、護士、及其他醫療人員更快速地了解患者的身理狀況，並提供適當的醫療服務。

結合完整身分認證的個人健康紀錄系統，除了能讓醫療服務提供者更快速的確認使用者的健康狀態，更重要的是能夠保護用戶的個人隱私與敏感資料。本文中，智慧卡用於儲存需要驗證的資訊與參數，並使用以雙線性配對為基礎的加密系統來驗證使用者身分的合法性。一個完整的身分驗證階段能夠使醫護人員在存取患者資訊時，同時能夠保護患者的隱私與安全。用來登錄個人健康照護系統的使用者密碼必須保證是安全與可靠的，不會被有心人士惡意攻擊而被破解，並能防範針對系統的安全性之攻擊。從上一章安全性分析中可以得證，本文所提出的身分認證機制可以有效抵禦常見的偽造合法使用者的攻擊手法、或是重送攻擊、其他多種密碼猜測的攻擊方法，以及藉由盜取驗證資訊來登入系統等常見的攻擊手法。

# 參考文獻


[1] Miller, RH. and Sim, I. (2004). Physician's use of electronic medical records: barriers and solutions, *Health affairs*, 23(2), 116-126. doi:10.1377/hlthaff.23.2.116

[2] Tang PC., Ash JS., Bates DW., Overhage JM., Sands DZ. (2006). Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption, *Journal of American Medical Informatics Association*, 13(2), 121– 26. doi: 10.1197/jamia.M2025

[3] Sittig, D. (2002).Personal health records on the internet: a snapshot of the pioneers at the end of the 20th Century. *International Journal Medical Informatics*, *65*(1), 1-6. doi: 10.1016/S1386-5056(01)00215-5

[4] Tang P.C. and Newcomb, C. (1998). Informing Patients: A Guide for Providing Patient Health Information. *Journal of American Medical Informatics Association*, *5*(6), 563-70. doi: 10.1136/jamia.1998.0050563

[5] American Medical Informatics Association and the American Health Information Management Association (2007).The Value of Personal Health Records: Joint Position Statement for Consumers of Health Care. *Journal of American Medical Informatics Association*, *78*(4), 22-24.

[6] Connecting for Health Personal Health Working Group (2003). The Personal Health Working Group Final Report, John and Mary R., Markle Foundation. Connecting for Health.

[7] AHIMA e-HIM Personal Health Record Work Group (2005). Defining the personal health record, AHIMA releases definition, attributes of consumer health record, *Journal of American Medical Informatics Association*, *76(*6), 24-5.

[8] Margaret Rouse (2010), Google Health, S*earchHealthIT*, DIALOG, Available: https://searchhealthit.techtarget.com/definition/Google-Health, April 09.

[9] Margaret Rouse (2010), Microsoft HealthVault, S*earchHealthIT*, DIALOG, Available: https://searchhealthit.techtarget.com/definition/Microsoft-HealthVault, May 01.

[10] Jordan T. Cohen (2009), HIPAA, The HITECH Act, and How Google May Still Be Able to Distribute and Profit From, Your Personal Health Info, *HealthReformWatch*, DIALOG, Available: http://www.healthreformwatch.com/2009/08/06/hipaa-the-hitech-act-and-how-google-may-still-be-able-to-distribute-and-profit-from-your-personal-health-info/, August 06.

[11] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov and M. Ylianttila (2014), Two-phase authentication protocol for wireless sensor networks in distributed iot applications, Paper presented at 2014 IEEE Wireless Communications and Networking Conference, Istanbul, Turkey, April 6-9.

[12] R. Amin, G. P. Biswas (2015). Design and Analysis of Bilinear Pairing Based Mutual Authentication and Key Agreement Protocol Usable in Multi-server Environment, *Wireless Personal Communications*, *84*(1), 439–462. doi: 10.1007/s11277-015-2616-7

[13] Luigi Atzori, Antonio Iera and Giacomo Morabito (2010). The Internet of Things: A survey, *Computer Networks*, 54(15), 2787-2805. doi: 10.1016/j.comnet.2010.05.010

[14] Somayya Madakam, R. Ramaswamy, Siddharth Tripathi (2015).Internet of Things (IoT): A Literature Review, *Journal of Computer and Communications*,3(5), 164-173. doi: 10.4236/jcc.2015.35021

[15] A. Shamir (1984). Identity-Based Cryptosystems and Signature Schemes, *Advances in Cryptology-Proceedings of Crypto*, *196*, 47–53. doi: 10.1007/3-540-39568-7-5

[16] Dan Boneh and Matt Franklin (2001). Identity-based Encryption from the Weil Pairing, *Advances in Cryptology-Proceedings of Crypto*, *2139*, 213–229. doi:

10.1007/3-540-44647-8_13

[17] A. Joux (2002). The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems, *International Algorithmic Number Theory Symposium*, *Springer-Verlag*,*2369*, 20-32. doi: 10.1007/3-540-45455-1_3

[18] D.C. Kaelber, A.K. Jha, D. Johnston, B. Middleton and D.W. Bates (2008). A research agenda for personal health records (PHRs), *Journal of the American Medical Informatics Association*, *15*(6), 729-736. doi: 10.1197/jamia.M2547

[19] Ali Sunyaev, Dmitry Chornyi, Christian Mauro and Helmut Krcmar (2010). Evaluation Framework for Personal Health Records: Microsoft HealthVault Vs. Google Health, Paper presented at2010 43rd Hawaii International Conference on System Sciences, Honolulu, HI, USA, Jan 5-8.

[20] M.I. Kim and K.B. Johnson (2002). Personal Health Records: Evaluation of Functionality and Utility, *Journal of American Medical Informatics Association*, *9*(2), 171-180. doi: 10.1197/jamia.M0978

[21] N. Archer, U. Fevrier-Thomas, C. Lokker, K.A. McKibbon, S.E. Straus (2011). Personal health records: a scoping review, *Journal of the American Medical Informatics Association*, *18*(4), 515-522. doi: 10.1136/amiajnl-2011-000105

[22] G. Eysenbach (2001). What is e-health, *Journal of medical internet research*, *3*(2), e20.doi:10.2196/jmir.3.2.e20.