Communications of the CCISA
Vol. 26 No. 2 May. 2020

具有網路安全性保護之智慧藥盒

陳勇勝[1]、匡融成[1]、廖麒先[1]、吳信德[2]
國立澎湖科技大學資訊工程系[1]
國立宜蘭大學資訊工程系[2]
[2]hsinte@niu.edu.tw

摘要

「遵從醫囑」對慢性病患者來說，相當重要，而在「服藥遵從性不良」行為者，又為老人偏多，於是我們想出了利用智慧手機搭配智慧藥盒監督與提醒用戶。因考量到用戶多數為老年者不熟悉 APP 的操作流程，本文還加入電子藥單的即時傳送，讓用戶有簡便的使用環境及節省設定上的麻煩。

這套系統先通過醫生診斷完畢,透過醫生手機 APP 將電子藥單由 NFC 傳送至用戶端(病人)APP 並進行設定服藥時間及回診倒數天數等資訊，當到了服藥時間到由手機 APP 啟動鬧鈴提醒用戶服藥。在智慧藥盒的部份我們利用 Arduino UNO 開發板來控制，並在控制板加上時間 RTC 時鐘模組來掌控時間，當到了服藥時間伺服馬達會啟閉取藥口。另外這些資料有病患個資問題，因此需要安全性傳輸與安全性驗證確保個資的安全性。

關鍵詞：智慧藥盒、物聯網、雙線性加密

Communications of the CCISA
Vol. 26 No. 2 May. 2020

Smart Pillboxes with Network Security

Yong-Sheng Chen[1], Rong-Cheng Kuang [1], Chi-Hsien Liao [1],Hsin-Te Wu[2]
Department of Computer Science and Information Engineering, National Penghu University of Science and Technology, Taiwan.[1]
Department of Computer Science and Information Engineering, National Ilan University, Taiwan.[2]
[2]wuhsinte@gms.npu.edu.tw

Abstract

"Medical Compliance" is a critical concept to chronic patients; among which, the elderly make up a high proportion to poor medication adherence. Therefore, we developed a mobile application to work with the smart pillbox for supervising and reminding users. On the other hand, considering that most elderly users are not acquainted with the operation of mobile applications, the application also added an instant delivery function for electronic prescriptions, which provides a user-friendly operation environment and saves the troublesome setting process.

After seeing a doctor, the doctor could deliver the electronic prescription through the application to the patient via Near Field Communication (NFC). Additionally, users can set medication times and the return visit countdowns on the application, so that the application will ring the alarm to remind patients taking medicines. For the smart pillbox, we utilize Arduino UNO development board to control the system and add a Real-Time Clock (RTC) module to manage the time; the servomotor will open the lid when the patient needs to take medicines. Moreover, due to the personal information of patients, the system requires secure transmission and security verification for ensuring personal data protection.

Keywords: Smart Pillboxes、Internet of Things、Bilinear Pairing

壹、前言

現今許多國家都邁向高齡化社會，許多高齡者都有慢性病等問題，因此需要定期回診以及服藥等情況，並且許多高齡者有獨居或者子女需工作等情況，高齡者在看診時有時對於藥物或者回診時間了解性不足，因此有「服藥遵從性不良」的情況發生，現今高齡者的相關輔具產品非常多,但需要考量以下情況發生: 1.高齡者對於資訊科技的不適應性、2.穿戴式裝置的耗電量以及維護、3.高齡者的隱私，許多輔具產品功能太多，但對於高齡者而言是一大負擔，主要是高齡者需要高專注操作與學習，輔具產品屬於高移動性，因此需要使用電池進行電力使用，但如果電池續航力不足會導致高齡者要不斷進行電力補充，輔具產品都有高齡者相關資訊，這些醫療資訊與個資屬於敏感性資訊，因此需要密碼學技術保護安全性。

在文獻[12]提出現今高齡者照護方式已逐漸加重於有品質的在地老化，許多高齡者都選擇在家照護[7]，但如何確保在家居住的安全也是一大問題，因此需要輔助科技進行協助才行。任何長者適當的運動有助身體健康，但是許多長者有服藥的問題，雖然目前已有開發電子智慧藥盒產品，主要功能是提醒老年人用藥、記錄用藥時間以及提醒藥盒置放位置，如果智慧藥盒可以記錄老年人服藥前、後的身體健康指數，以提供醫生在看診時了解服藥的身體狀況，適當調整藥物的數量或者服用的時間，另外，許多藥物都有副作用或忌食的部份，在長者服用藥物前、後會告知藥物的副作用及忌食的部份，有些長者都有緊急藥物，例如:高血壓或氣喘藥物等，當開啟緊急藥物藥盒時會用簡訊通知家人，在服藥後身體健康指數會進行分析，例如:血壓瞬間下降太低，可能會有昏倒情況發生，會簡訊通知家人並發出警訊讓長者注意身體狀況。

許多長者需要服用慢性病藥物，由於藥物服用時間以及數量不同，而長者在服藥上有可能會混淆或者忘記服藥，所以已經有智慧型藥盒產品，主要是用來提醒長者服藥並且記錄用藥時間，但是我們關注的是長者服藥前、後的生理資訊，因為這些資訊可提供醫生在診斷時調整長者的藥物,另外,許多藥物都會有副作用或忌食的情況,在服藥前、後可以透過穿戴式裝置提醒長者注意，在服藥後，如果分析生理資訊有異常會透過智慧型手機簡訊通知家人，有些長者有緊急用藥，例如:高血壓、氣喘等藥物，當長者在藥盒使用緊急藥物時也會主動簡訊通知家人,如此,我們希望藥盒的功能不僅只是提醒功能，而是能夠了解長者在服用藥物時生理資訊，這些生理資訊可以讓醫生很能夠掌握長者的生理狀況。

本文提出智慧藥盒主要結合 APP 與實際藥盒,並且利用 Bilinear Pairing 技術進行身分驗證以及資料加密，確保資料的安全性以及身分驗證的合法性，本文提出的智慧藥盒主要提供功能如下: 1. 高齡者服藥提醒與紀錄、2.醫生電腦端藥物系統、3.家屬端藥物資訊系統、4.智慧藥盒，醫生開立相關藥物資訊會利用電腦端藥物系統傳遞到家屬端藥物資訊系統，家屬可以從藥物資訊系統了解藥物服藥資訊，並且資訊系統可以與智慧藥盒進行資訊同步，本文提出的方法都利用 Bilinear Pairing 進行加解密保護，並且可以進行

雙方身分驗證，確保雙方是合法使用者。

貳、文獻探討

目前逐漸有許多相關居家安全防護系統[9]、長期健康監控系統[15]以及緊急通報系統[14]，但這些系統都需要考量到高齡者操作認知，以及高齡者的攜帶性，另外，許多文獻[5]透過感測器、iBeacon 等進行行為分析以及活動範圍偵測，這些資訊都沒受到網路安全或資訊安全保護，許多資訊直接暴露在系統上或者遭到非法人士竊聽，感測器越多並且偵測間隔越小耗電量越大，任何感測器裝置都需要考量到電池維護問題[13]。

在文獻[2]中主要透過 Pedestrian Dead Reckoning 以及行動裝置中的感測器進行室內定位，由於行動裝置中有許多感測器，例如 Accelerometer Sensor、Gyroscope 等感測器，利用行動裝置感測器的數據進行 Pedestrian Dead Reckoning 演算法計算，例如:行走速度、行走距離等，並結合 iBeacon 範圍定位確認使用者在室內的位置，文獻[8]方法使用行動裝置中的感測器以及 iBeacon 硬體價格較低，並不需要大量設置 Passive Infrared Sensor 進行室內定位偵測，文獻[8]在模擬實驗結果中有不錯的成果。在文獻[8]主要提出在三個 Beacon 範圍中，利用接收到 Beacon 的訊號強弱以及訊息時間，透過 triangle localization 計算，判斷使用者目前位置，文獻[10]在模擬結果方面，與其他方法進行模擬在定位誤差的估算比較小，文獻[1][3][4][16]主要提出利用 RFID 感測進行老人活動偵測，在高齡者衣服裝上 RFID Tag 以及身上攜帶 RFID Reader，在室內裝置 UHF RFID Reader，並收集高齡者不同位置以及不同活動狀態中 RFID 的 Received Signal Strength (RSS)，再透過 support vector machine 進行學習與分類訊號以及行為，當手機收到 RFID 的 Received Signal Strength 時就可以判斷高齡者目前行為以及位置，由於上述方法主要是定位高齡者的室內位置，並且需要行動裝置、RFID 等設備，但這些設備對於高齡者而言攜帶性以及操作性會有困擾，例如:電池維護等，本文在定位部份主要調整 Beacon 功率、Received Signal Strength 與狀態機進行定位，降低感測器設置數量以及硬體成本。

參、技術介紹

3.1. 系統介紹

本文提出的系統環境如圖 1 所示，醫生可以從電腦系統中輸入高齡者藥物資訊以及回診時間，家人可以從手機資訊系統查看高齡者服藥資訊以及回診時間，另外可以利用智慧手機與智慧藥盒進行服藥資訊同步，智慧藥盒會定時提醒高齡者進行服藥。

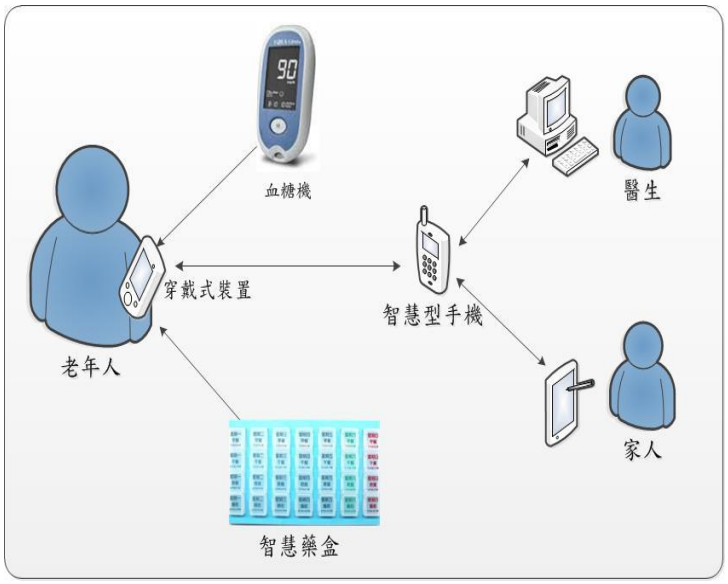


圖 1、智慧藥盒示意圖

3.2. Bilinear Pairings

本文使用 Bilinear Pairings 技術建構網路安全系統，Bilinear Pairings 可將 elliptic-curve discrete logarithm 對應到一個有限體上的離散對數問題，假設 G_1 和 G_2 are, 代表加法群與乘法群，q 代表為質數，假設 P,Q 是 G_1's generator 以及 bilinear mapping 為 $e:G_1\times G_1\to G_2$.，bilinear pairing 定義如下:

(1) Bilinear: $e=(aP,bcP)=e(P,P)^{abc}$, $e(a\cdot P+b\cdot P+c\cdot P,P)=e(a\cdot P,P)e(b\cdot P,P)e(c\cdot P,P)$, for all $P\in G_1$ and $a,b,c\in Z_q^*$.

(2) Non-degeneracy: $Q\in G_1$ such that $e(Q,Q)\neq 1$.

(3) Computable: There exists an efficient algorithm to compute $e(Q,Q)$ for all $Q\in G_1$.

在[6][11]中有實現 Bilinear Pairings 加密技術，並且 G_1 與 q 的資料量各為 161 bits 以及 160 bits。

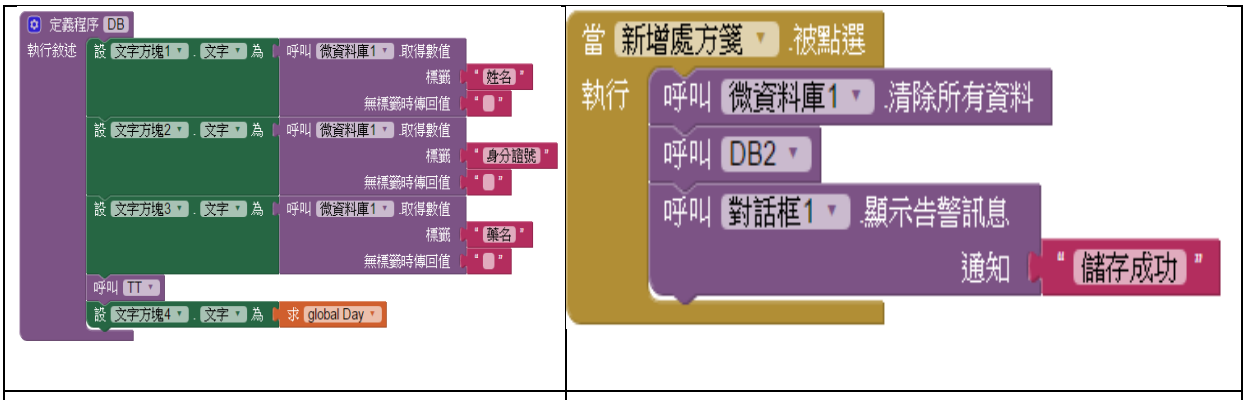
肆、方法

4.1 系統加密技術

本文利用 Bilinear Pairings 加密技術建置 Public Key Infrastructure 機制，假設醫生每一單位都有 PK_{ID_D} 、 PR_{ID_D} 、 PU_{ID_D} 、 ID_D ，當醫生想存取病患的資訊時，會發出訊息 $PK_{ID_F}\left(PR_{ID_D}\left(S\right)\right)$ 給病患進行驗證，病患利用解密後，並且利用 S 當作雙方私密金鑰進行私密通訊，其中 SE 為對稱式加密，病患會利用對稱式加密進行訊息加密後傳送給醫生端，

4.2 醫生端資訊系統

本文從紀錄病患資料、傳送吃藥時間與吃藥的天數資料進行系統設計，並且結合資料庫進行病患的相關資料存取，如圖 2a 所示，醫生將病患的資訊從資料庫取出，如圖 2b 所示，醫生可以開立病患的處方簽，並儲存資料庫中。

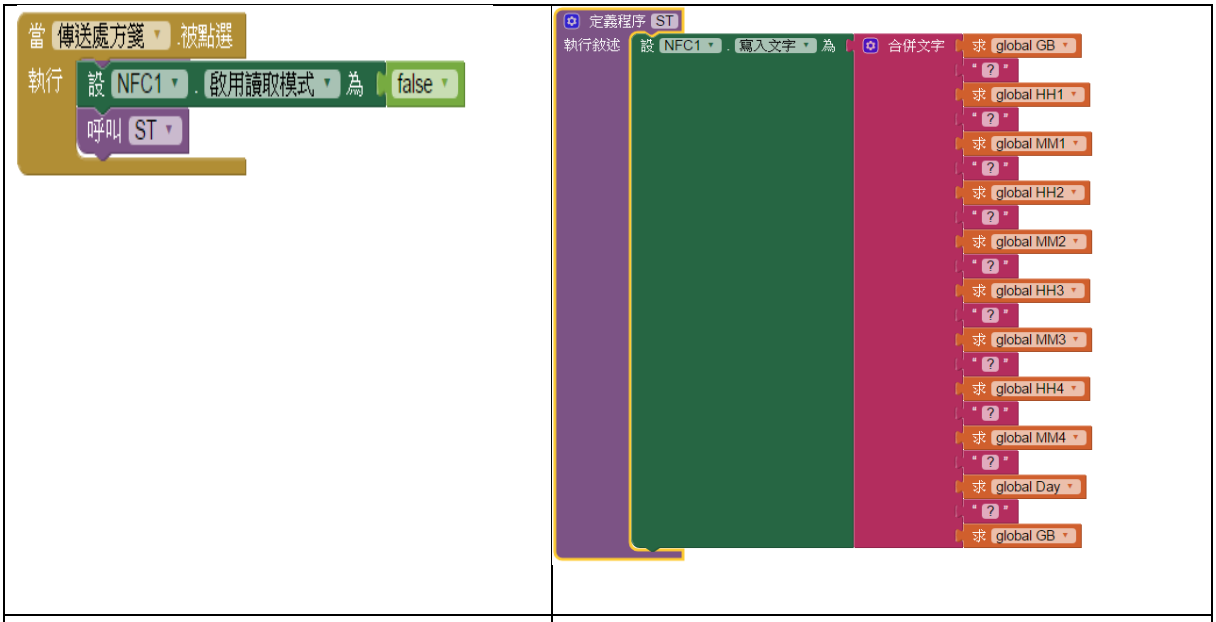


a. 資料庫存取病患資料	b. 新增處方簽

圖 2、醫生端開發系統

4.3、病患家屬資訊系統

系統提供顯示目前的時間，鬧鐘設定提醒自己吃藥時間到了、吃藥的天數提醒自己哪時該回診、與藥盒藍芽連線記錄吃藥時間與藥盒狀態和以 NFC 接受吃藥時間、吃藥的天數並且直接設定，如圖 3 所示，寫入至資料庫中並且利用 NFC 進行資料傳輸。



a. 傳送　　b. 傳送資訊寫入 NFC

圖 3、家屬病患資訊系統寫入流程

伍、實驗結果

目前市面上嵌入式微處理器的開發板品種總量已經超過 1000 多種，像是 Arduino、Raspberry Pi、Nano PI…等等。經分析此專題所需功能後選擇 Arduino UNO 開發板製作藥盒，選擇使用 Arduino 是因為目前市面上已有許多開發成熟且穩定的模組可進行實驗，Arduino 軟體開發環境方面使用 C 語言進行編譯，故較方便簡潔、靈活、便宜。此藥盒主要的功能用道微動開關跟舵機控制藥盒開起跟關閉、用藍芽晶片回傳到手機 APP 紀錄服藥時間和藥盒開或關、用 RTC 時間模組判斷七個藥盒使用哪一個，本文使用軟硬體設備如表 1 所示，本文實驗結果如圖 4 所示。

表 1、軟硬體設備

硬體: 1.Arduino UNO 開發板 2.舵機 3.RTC 時鐘模組 4.藍芽晶片 元件: 1.電阻 2.微動開關	軟體: 1.Arduino UNO 開發板的內建開發環境 (C 語言) 2. AppInventor

a. 戶端提醒時間設定

b. 鬧鐘提醒時間到時

圖 4、實驗結果

陸、結論

如能藉由智慧型手機的便利搭配本智慧型藥盒由手機輕易的設定服藥的時間，當時間一到，智慧型手機便會自動的提醒且藥盒一天只能開一個，相信必能改善病患時常忘記服藥與服錯藥的困境。未來會加入更多輔具，讓高齡者居家生活以及健康更加便利，並且讓獨居高齡者透過輔具能夠提升生活品質。

參考文獻

[1] Eva Arias-de-Reyna, and Petar M. Djuri´c, “Indoor Localization With Range-Based Measurements and Little Prior Information”, IEEE Sensors Journal, Volume: 13, Issue: 5, May 2013.

[2] G.-Z. Yang and M. Yacoub, Body Sensor Networks. New York, NY, USA: Springer, 2006.

[3] L. Lorenzen-Huber, M. Boutain, L. J. Camp, K. Shankar, and K. H. Connelly, “Privacy, technology, and aging: A proposed framework,” Ageing Int., vol. 36, no. 2, pp. 232–252, 2011.

[4] Liang Wang, Tao Gu, Xianping Tao, and Jian Lu, “Toward a Wearable RFID System for Real-Time Activity Recognition Using Radio Patterns”, IEEE Transactions on Mobile Computing, Volume 16 Issue 1, January 2017.

[5] M. E. Pollack, L. Brown, D. Colbry, C. E. McCarthy, C. Orosz, B. Peintner, S. Ramakrishnan, and I. Tsamardinos, “Autominder: An intelligent cognitive orthotic system for people with memory impairment,” Robot. Auton. Syst., vol. 44, no. 3, pp. 273–282, 2003.

[6] M. Scott, “Computing the tate pairing,” in Proceedings of the Cryptographers’ Track at the RSA Conference, 2005, pp. 293–304.

[7] N. Farber and D. Shinkle, “Aging in place: A state survey of livability policies and practices,” AARP Research Rep., Dec. 2011. [Online]. Available: https://assets.aarp.org/rgcenter/ppi/liv-com/aging-in-place-2011-full.pdf.

[8] N. Farber and D. Shinkle, “Aging in place: A state survey of livability policies and practices,” AARP Research Rep., Dec. 2011. [Online]. Available: https://assets.aarp.org/rgcenter/ppi/liv-com/aging-in-place-2011-full.pdf.

[9] Neal N. Xiong, Wenliang Wu, Chunxue Wu, Hongju Cheng, "An Improved Node Localization Algorithm Based on Positioning Accurately in WSN," Journal of Internet Technology, vol. 20, no. 5 , pp. 1323-1332, Sep. 2019.

[10] P. Barberger-Gateau, D. Commenges, M. Gagnon, L. Letenneur, C. Sauvel, and J.F. Dartigues, “Instrumental activities of daily living as a screening tool for cognitive impairment and dementia in elderly community dwellers,” J. Amer. Geriatr. Soc., vol. 40, no. 11, pp. 1129–1134, 1992.

[11] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, “Proceedings of the 22nd annual international cryptology conference,” in Proceedings of the Cryptographers Track at the RSA Conference, 2002, pp. 354–368.

[12] Siou-Jyun Lin and Wan-Yu Sie, “A Probe into the Safety of Science and Technology in the Safety of the Elderly”, Taiwanese Gerontological Forum, VOL: 17, 2013.

[13] T. Lee and A. Mihailidis, “An intelligent emergency response system: Preliminary development and testing of automated fall detection,” J. Telemed. Telecare, vol. 11, no. 4, pp. 194–198, 2005.

[14] T. Mythili, J. Ramesh, P. Ramanathan, "Innovative Localization Algorithm Using the Line of Intersection Technique in Wireless Sensor Networks," Journal of Internet Technology, vol. 21, no. 2 , pp. 425-433, Mar. 2020.

[15] Wook Song, HwaMin Lee, Seung-Hyun Lee, Min-Hyung Choi, Min Hong, "Implementation of Android Application for Indoor Positioning System with Estimote BLE Beacons," Journal of Internet Technology, vol. 19, no. 3 , pp. 871-878, May. 2018.

[16] Zhenghua Chen, Qingchang Zhu, and Yeng Chai Soh, “Smartphone Inertial Sensor-Based Indoor Localization and Tracking With iBeacon Corrections”, IEEE Transactions on Industrial Informatics, Volume: 12, Issue: 4, Aug. 2016.