適用於電子醫療系統的資料存取安全機置

王孟穎[1]　洪國寶[2]　陳國璋[3]　蘇旻姿[4]
國立中興大學資訊科學與工程學系[1,2,3,4]
TWISC@NCHU[1,2,4]
melody26613@gmail.com[1]
gbhorng@cs.nchu.edu.tw[2]
s9756013@csmail.nchu.edu.tw[3]
g104056024@mail.nchu.edu.tw[4]

摘要

物聯網與雲端蓬勃發展，其應用包括醫療、經濟及社群網路，滿足人類生活上的種種需求。也由於這樣的發展，各式的個人資料及資訊流通於不同的裝置與平台，其中醫療的資訊又更為隱私，本篇論文將探討如何在電子醫療的環境下，保障資料提供者(以下簡稱使用者)的隱私安全。考量到使用者的隱私安全，我們將以下需求列為電子醫療中必有的安全機制，第一，使用者、雲端伺服器及資料消耗者(以下簡稱醫生)間有安全的傳輸機制來傳送資料。第二，雲端伺服器能夠認證要存取資料的醫生。第三，要在半可信的雲端伺服器系統保障使用者的資料隱私。本篇論文提出符合以上需求的方法，使用 Elgamal 私鑰分割來完成使用者及醫生間的秘密分享。

關鍵詞：電子醫療、隱私、安全、Elgamal 私鑰分割

1. 前言

在物聯網環境中包含了終端感測裝置、智慧行動裝置、後端雲端伺服器。在這樣的環境架構底下，須考量到的安全層面有以下幾點[1][2]。(一)終端裝置及行動裝置資安問題：存取控制不當，設定被任意修改。缺乏嚴謹的資料保護機制，隱私的感測資料沒有被加密保護。預設密碼以及後門程式讓終端裝置被侵入。(二)通訊媒介資安問題：資料傳輸過程中，在 TCP/IP 個通訊層中傳送，層層傳遞到伺服器前，封包中途被攔截暴露隱私。以及(三)後端系統資安問題。本文的目標為，在物聯網環境下的電子醫療服務中，保護使用者的醫療感測資料安全。

1.1 環境架構

本文假設的行動醫療架構[3]如圖 1 所示。主要有四個角色，首先是使用者，本文假設使用者會用以下醫療感測裝置：血糖感測、體重計、血壓計，醫療感測裝置測量完使用者身體資訊後，會將感測資料上傳至使用者手機，使用者手機收到醫療感測資料後，再將資料加密上傳雲端。

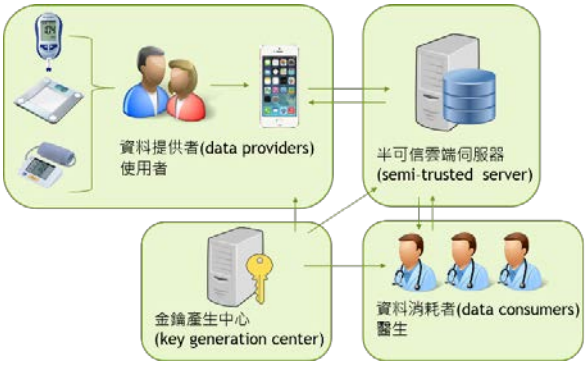

圖 1 環境架構

其次是雲端伺服器，本文假設此伺服器為半可信狀態，即此伺服器會保護資料不被惡意外來者所存取，但此伺服器可能會在使用者未授權情況下監控使用者資料。伺服器會將使用者及醫生連線存取資料的紀錄留存在 log 檔裡。

再來是醫生，醫生會透過雲端伺服器來取得使用者資料，並提供使用者相關的醫療諮詢與建議。

最後是金鑰產生中心，本文假設金鑰產生中心可完全信任。金鑰產生中心會產生公鑰私鑰對給伺服器、使用者及醫生。

1.2 各個角色屬性及行為

本文假設各個角色的屬性及行為如下，首先是使用者的屬性及行為。使用者的屬性有：使用者 ID、醫療感測資料、對稱式金鑰、使用者公鑰、使用者私鑰。其中，使用者 ID 是用來辨別使用者身分；對稱式金鑰是用來加密醫療感測資料；使用者公鑰及私鑰是用來分享資料存取權限。使用者的行為有：將感測資料上傳、經由伺服器授權讀取資料的權限給醫生、經由伺服器取消醫生讀取資料的權力、跟伺服器取得自己的相關感測資料。

其次是雲端伺服器的屬性及行為，伺服器

的屬性有：伺服器公鑰、伺服器私鑰，其存在的功能在於確保使用者與伺服器間、醫生與伺服器間有安全的資料傳輸機制。伺服器的行為有：接收及儲存使用者的感測資料、將醫生的資料權限要求轉傳給使用者、紀錄使用者及其相關授權醫生的 ID、使用者提出刪除醫生權限後，取消醫生權限、傳送感測資料給使用者、傳送感測資料給授權醫生。

最後是醫生的屬性及行為，醫生的屬性有：醫生 ID、醫生公鑰、醫生私鑰。可讓伺服器來認證醫生身分。醫生的行為有：經由伺服器對使用者提出讀取資料的要求、經由伺服器取得使用者醫療感測資料。

2 相關研究

2.1 Elgamal 公開金鑰加密法

本篇論文使用的公開金鑰加密法為 Elgamal 加密法，被 T. ElGamal [5]所發明，是一種公開金鑰加密系統，以下介紹 Elgamal 加密法的主要三個步驟：

1. 初始化：選定一質數p，再選出p的原根g，隨機產生私鑰X，X及g小於p，計算公鑰為$Y = g^X \ mod \ p$。其中$\{p, Y, g\}$為公開參數。
2. 加密：假設明文為m，加密前選定一亂數r。並計算
   $E_Y(m) = m \bullet Y^r \ mod \ p$。
3. 解密：計算
   $D_X(E_Y(m))$
   $= \ g^{-rx} \bullet E_Y(m) \ mod \ p$
   $= \ g^{-rx} \bullet (m \bullet Y^r \ mod \ p) \ mod \ p$
   $= \ g^{-rx} \bullet m \bullet \ (g^x)^r \ mod \ p$
   $= m \ mod \ p$
   $= m$

2.2 Elgamal 私鑰分割

根據 A. Ivan [4]等人提出的方法，基於 Elgamal 加密法下的秘密分享技術，將 Elgamal 私鑰分割並分給不同角色即可達到秘密分享。將 Elgamal 私鑰X分割成兩部分，即$X = X_1 + X_2$，解密時先用其中一部分解密，再用另一部份解密即可得到原始明文。

1. 加密：
   $E_Y(\mathrm{m}) = m \bullet Y^r \ mod \ p$
2. 解密：
   $D_{X_2}\left(D_{X_1}\left(E_Y(m)\right)\right)$
   $= (g^{-r})^{X_2} \bullet D_{X_1}\left(E_Y(m)\right) \ mod \ p$
   $= (g^{-r})^{X_2} \bullet (g^{-r})^{X_1} \bullet E_Y(m) mod \ p$
   $= (g^{-r})^{X_1+X_2} \bullet E_Y(m) \ mod \ p$
   $= (g^{-r})^{X} \bullet E_Y(m) \ mod \ p$
   $= D_x(E_Y(m))$
3. 範例：
   選定一質數$p = 23$，選取質數p一原根$g = 11$，隨機亂數$r = 3$，明文$m = 10$。私鑰$X = 6$，分割$X = X_1 + X_2$，$X_1 = 2$，$X_2 = 4$，計算公鑰 $Y = g^X \ mod \ p = 11^6 \ mod \ 23 = 9$。

加密：

$E_Y(\mathrm{m})$
$= m \bullet Y^r \ mod \ p$
$= 10 \bullet 9^3 \ mod \ 23$
$= 22$

解密：

$D_{X_1}(E_Y(m))$
$= \ g^{-rX_1} \bullet E_Y(m) \ mod \ p$
$= \ 11^{-3*2} \bullet 22 \ mod \ 23$
$= 5$
$D_{X_2}\left(D_{X_1}\left(E_Y(m)\right)\right)$
$= (g^{-r})^{X_2} \bullet D_{X_1}\left(E_Y(m)\right) \ mod \ p$
$= 11^{-3*4} \bullet 5 \ mod \ 23$
$= 10$

3 本文方法

本文方法參考 D. Thilakanathan 等人[7]使用對稱式金鑰來加密資料，再透過 Elgamal 公開金鑰來加密對稱式金鑰，並運用 Elgamal 私鑰分割來達到使用者分享資料存取權限給醫生。其中，同一位使用者分享給不同醫生的部分私鑰皆不同，保障使用者資料存取的安全性。並配合智慧感測裝置與手機的連線與否來決定應用程式是否可解鎖，以防使用者手機丟失，資料被外人存取的狀況。

為了滿足電子醫療環境使用者需求，本文方法分成多個步驟：使用者註冊、使用者上傳資料、使用者或醫生身分認證、使用者資料存取權限分享、醫生取得資料、取消醫生存取資料權限、緊急情況下使用者與醫生直接聯繫。

3.1 初始化

初始化階段，金鑰產生中心產生公鑰Y、私鑰X、醫生 ID。如圖 2 所示。

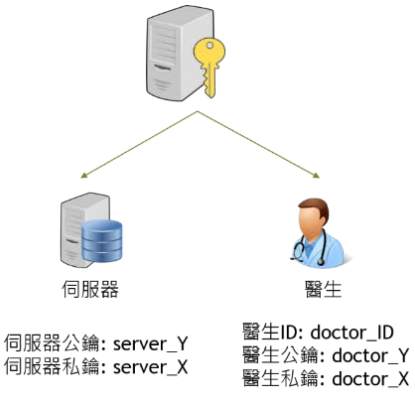

圖 2 初始化

3.2 使用者註冊

使用者註冊階段，使用者提出註冊請求，並上傳使用者姓名、電子信箱到伺服器。伺服器接收請求後，將訊息轉傳給金鑰產生中心產生使用者 ID、使用者公私鑰，產生使用者 ID 及公私鑰後回傳給使用者。使用者接收到 ID 及公私鑰後，分割私鑰X，$X = X_1 + X_2$，使用者將X_1分享給伺服器，以便之後分享資料存取權限。如圖 3 所示。

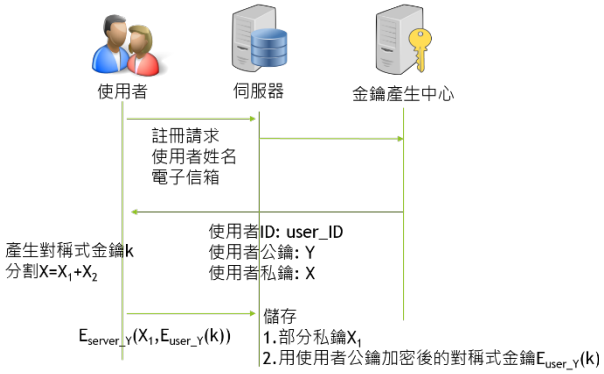

圖 3 使用者註冊

3.3 使用者上傳資料

使用者的智慧感測裝置感測資料後，將資料傳至使用者手機，使用者手機先使用對稱式金鑰 k 加密感測資料，再使用伺服器公鑰加密後上傳資料，儲存在雲端伺服器。如圖 4 所示。

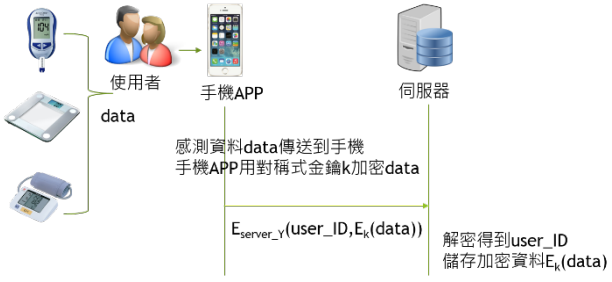

圖 4 使用者上傳資料

3.4 使用者或醫生身分認證

使用者(或醫生)向伺服器提出連線需求，伺服器產生一亂數r，用使用者(或醫生)的公鑰加密後回傳挑戰，使用者(或醫生)用私鑰解密後計算$r + 1$回傳給伺服器，伺服器驗證收到的資料是否為$r + 1$。如圖 5 所示。

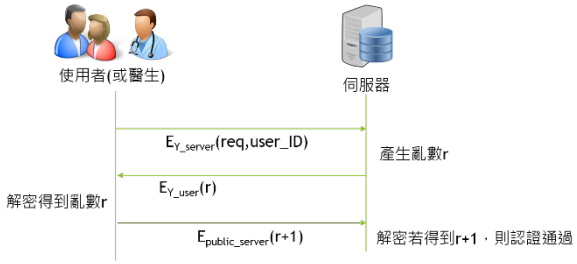

圖 5 使用者或醫生身分認證

3.5 資料存取權限分享

醫生向伺服器提出對指定使用者的資料存取要求，伺服器轉傳請求給指定使用者，使用者同意後將私鑰X_2分割，即$X_2 = X_3 + X_4$，其中X_3分享給伺服器、X_4分享給醫生。如圖 6 所示。

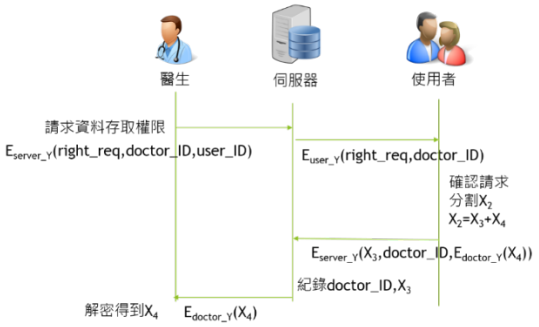

圖 6 資料存取權限分享

3.6 醫生取得資料

擁有資料存取權限的醫生，向伺服器提出取得資料的需求後，伺服器傳送用X_1、X_3部分解密的對稱式金鑰 k 以及用 k 加密的資料回傳給醫生，醫生使用自己擁有的X_4將 k 解出，再用 k 解密即可獲得使用者的感測資料，醫生取得資料後，可透過伺服器將相關醫療建議傳給使用者。如圖 7 所示。

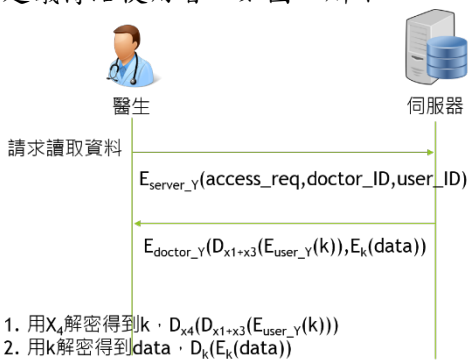

圖 7 醫生取得資料

3.7 取消醫生存取資料權限

使用者可取消醫生權限，只要給伺服器

醫生的 ID，伺服器會在使用者合法存取名單裡刪除該醫生 ID，並刪除醫生擁有的部分私鑰X_4。如圖 8 所示。

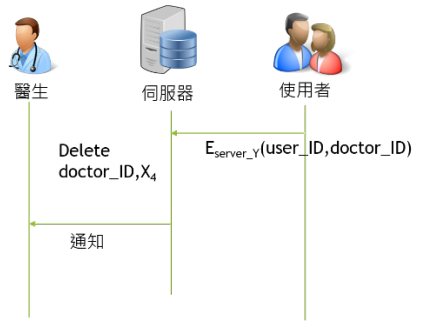

圖 8 取消醫生存取資料權限

3.8 緊急情況下使用者與醫生直接聯繫

緊急情況下，使用者與醫生可直接連線做醫療診斷或相關醫療措施。

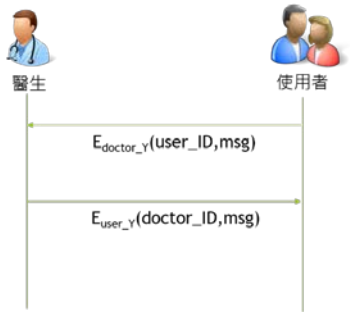

圖 9 緊急情況

3.9 Elgamal 私鑰分割架構

本文方法將用來加密對稱式金鑰的 Elgamal 私鑰分割成 4 部分，一共 2 步驟。第 1 步驟將X分割成 2 部分$X = X_1 + X_2$，其中X_1分享給伺服器。第二步驟將X_2隨機分割成 2 部分$X_2 = X_3 + X_4$，X_3分享給伺服器、X_4分享給醫生。其中，不同的醫生將擁有不同的X_4，且伺服器及醫生將沒辦法擁有完整的 Elgamal 私鑰，無法解密使用對稱式金鑰加密的感測資料。私鑰分割架構如圖 10 所示。

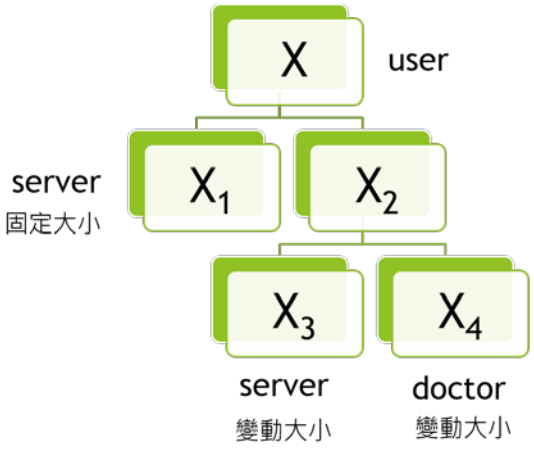

圖 10 私鑰分割架構

4 分析比較與討論

4.1 效能與安全性分析

本篇文章達到以下之安全性

1. 資料權限分享

透過將私鑰解密分享給伺服器與醫生來達成，醫生及伺服器皆不能夠單獨解開資料。其中，同一個使用者，對不同醫生分享資料時，分享的部分私鑰皆不同，保障資料的安全性。

2. 內部攻擊

本文中的每一階段都沒有讓伺服器得到解密的資料，每一階段傳送資料或儲存資料時，資料皆保持加密的狀態，確保使用者的資料不被半可信伺服器所洩漏。

3. 撤銷存取權限

本文方法中，使用者擁有撤銷醫生存取資料的權限，使用者僅需透過伺服器將醫生得到的部分私鑰刪除，即可完成撤銷醫生存取資料權限的功能。

4. 認證

本文提供身分認證的方法，確保進出系統的醫生及使用者是經過註冊的身分，也確保資料被存取的安全性。

5. 安全傳輸通道

資料透過公開金鑰系統加解密傳送，確保資料不會洩漏給中間攔截者。

6. 手機丟失

本文中，透過判斷感測裝置與手機的連線與否，來決定使用者電子醫療應用程式是否可解鎖。即使手機丟失被第三者所撿走，第三者也沒有感測裝置可解鎖手機，保障使用者資料不會洩漏。

4.2 比較與討論

根據 Kahani 等人[6]所提出的認證與存取控制機制，其重點著重在醫生的身分認證與資料存取上。文章中身分認證使用公開金鑰系統，本文取其公開金鑰系統做身分認證的機制。而其存取控制主要著重在資料庫管理。

根據 Thilakanathan[7]等人的方法，可以達到感測器、使用者手機、雲端伺服器之間安全的資料分享，文章將使用者私鑰分割成 4 個部分，分割 2 次，但使用者端將資料加密後，使用者又使用私鑰第 1 部分作解密再儲存在雲端，看似私鑰的第 1 部分並沒有完全的發揮功用。

根據 Sliva 等人提出的資料分享方法[8]，

對稱式金鑰系統與公開金鑰系統各有其優點，文章中在電子醫療環境下各提出對稱式金鑰系統的資料分享機制與公開金鑰系統的資料分享機制。而本文各取兩者的優點，使用對稱式金鑰將資料加密，並使用公開金鑰系統將對稱式金鑰加解密。

THEWS 架構是 Routsalanien[9]等人所提出，提出一個隱私資料保護架構，在使用者端上只擁有極少權限，伺服器掌管整個系統，在伺服器端與使用者間有著不對稱式的關係。而本文方法中，限制了伺服器的權限，保護使用者的隱私在半可信的伺服器下也不會顯露。

CREDENTIAL 架構是由 Felix Horandner 等人[10]所提出，文章中使用 proxy re-encryption 概念，在物聯網的各個領域：電子醫療、電子經濟系統、行動政府系統應用分享祕密資訊，文章中在醫生跟伺服器取得資料前，醫生跟使用者會直接連線，使用者使用醫生資訊產生相關分享金鑰，醫生再透過伺服器取得資料。而本文方法在使用者確認醫生存取資料請求之前，醫生與使用者不會有直接的連線，保障使用者的安全性。

表 1 相關文獻方法比較

方法	不同的分享對象有不同的金鑰	身分認證	資料加密後儲存在伺服器
[6]	V	V	
[7]			V
[8]			
[9]		V	V
[10]		V	
本文方法	V	V	V

5 結論

本文提出一個基於 Elgamal 私鑰分割之方法，用於電子醫療系統中使用者的醫療資料保護。本方法有以下特點，第一，不論是醫生或是伺服器，都不擁有完整的使用者私鑰，即使是伺服器也無法解密使用者的資料，保護使用者資料隱私。第二，醫生要先透過使用者授權，才可以透過伺服器得到完整的使用者感測資料，保障使用者的資料不被洩漏給未授權者。第三，每位醫生被分享到的部分私鑰都不同。第四，手機與使用者所有的感測裝置保持連線才能解鎖 APP，保障使用者即使手機弄丟，資料也不會洩漏。第五，擁有身份認證的機制。第六，資料及訊息傳輸過程中使用公開金鑰加密系統，保障傳輸中的資料能夠保持安全。第七，緊急情況時可讓使用者與醫生不透過伺服器直接聯繫，以節省時間，保障使用者生命安全。

致謝

本研究經費由科技部補助，計劃編號：MOST 105-2218-E-001-001。

參考文獻

[1] 莊祐軒、羅乃維，"物聯網安全的現況與挑戰"，***資訊安全通訊*** 19 卷 4 期，pp. 16-29，2013。

[2] S. Kraijak and P. Tuwanut, "A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends," ***2015 IEEE 16th International Conference on Communication Technology (ICCT)***, 2015, pp. 26-31.

[3] N. M. Shrestha, A. Alsadoon, P. W. C. Prasad, L. Hourany and A. Elchouemi, "Enhanced e-health framework for security and privacy in healthcare system," ***2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC)***, 2016, pp. 75-79.

[4] A. Ivan, Y. Dodis, " Proxy cryptography revisited. " ***In Proceedings of the Tenth Network and Distributed System Security Symposium***,2003.

[5] T.ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms. " ***Advances cryptology***, pp. 469 – 472, 1985.

[6] N. Kahani, K. Elgazzar, J. R. Cordy, "Authentication and Access Control in e-Health Systems in the Cloud" *2016 IEEE 2nd* ***International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)***, 2016, pp. 13-23.

[7] D. Thilakanathan, Y. Zhao, S. Chen, S. Nepal, R. A. Calvo and A. Pardo, "Protecting and Analysing Health Care Data on Cloud," ***2014 Second International Conference on Advanced Cloud and Big Data***, Huangshan, 2014, pp. 143-149.

[8] B.M. Silva, J.J. Rodrigues, F. Canelo, I.C. Lopes, L. Zhou, "A Data Encryption Solution for Mobile Health Apps in Cooperation Environments." ***J Med Internet Res***, 2013.

[9] P.S. Ruotsalainen, B. Blobel, A. Seppala, P.

Nykanen “Trust Information-Based Privacy Architecture for Ubiquitous Health.” ***JMIR Mhealth Uhealth***, 2013.
[10] F. Hörandner, S. Krenn, A. Migliavacca, F. Thiemer and B. Zwattendorfer, "CREDENTIAL: A Framework for Privacy-Preserving Cloud-Based Data Sharing," ***2016 11th International Conference on Availability, Reliability and Security (ARES)***, Salzburg, Austria, 2016, pp. 742-749.