應用具不可追蹤性的 RFID 於住院病人配藥安全之研究

李鴻璋*、傅俊崴**
*淡江大學資訊管理學系　副教授 hclee@mail.im.tku.edu.tw
**淡江大學資訊管理學系　研究生 2pac.westr@gmail.com

摘要

在台灣，2010 年醫療疏失事件中，藥物疏失事件位居第一，嚴重危害國人的醫療安全。會導致藥物疏失事件因素很多，例如藥名相似、配藥人員的疏失、藥物不良、…等，如何改善醫療疏失事件，目前已成醫療安全重要的課題。其中，如何將科技導入醫療體系中，以降低發生藥物失誤事件的機率，已成有效解決醫療誤置之重要選項，例如藥物與病人都擁有各自的 RFID 標籤，護士利用 RFID 的識別特性可以幫助識別病人身份與其藥物，以減少醫療錯誤的發生。在本論文中，我們建立安全用藥的 RFID 標籤雙向驗證機制，提供不可追蹤性並抵擋無線 RFID 標籤資訊外溢及其他攻擊行為，提供用藥資訊之不可否認性等，來提高用藥之準確性與安全性以保障病人權益。

關鍵字:RFID、藥物事件、住院病人、分配藥物。

A study of applying untraceable RFID for inpatient medication safety

Abstract

In Taiwan, medication errors which account for the major medical negligence incidentin 2010 would seriously endanger people's health care safety. There are many factors that induce the medication errors, such as the similar names among the drugs, the negligent dispensation of drugs,adverse drug problems,and so forth.How to apply information technology to improve medical malpractice has become an important research topic.To bulid RFID technology into the overall health behavior in order to reduce the occurrence of drug blunders or negligence of the dispensing staff has become a very important option for the medical malpractice. Examples are, drugs and patientshave their own RFID labels, nurse medical practices is certified by smart-card,and safe medical behavior is ensured and responded.

In this paper, based on RFID's identification of patients' identity and associated drugs, we further establish a two-way authentication mechanism and untraceable messages among the RFID tags,and thus,withstand malicious attacks. The dispensing process is undeniable and the responsibility is therefore established. All this can protect patients' rights and improve the environment and quality of the patient's medical.

Keywords:RFID、medical incidents、inpatient、medical malpractice。

1. 緒論

在醫療過程中，用藥錯誤是很重大的醫療疏失，嚴重的話可能會因此危及病人的生命安全。在美國，Hickner[3]短時間利用醫療回報系統，就收集了 507 份回報資訊，其中 357 份報告（佔 70%）只包括用藥錯誤，138 份報告（佔 27%）涉及藥物不良事件，12 份的報告（佔 2.4%）中兩者皆有。在我國，根據台灣病人安全通報系統 2010 年年報[8]，2010 年所接受之通報件數達 50,310 件，如圖 1，

年度	2005 年		2006 年		2007 年		2008 年		2009 年		2010 年	
序位	類別	件數(%)	類別	件數(%)	類別	件數(%)	類別	件數(%)	類別	件數(%)	類別	件數(%)
1	跌倒事件	747 (31.0%)	跌倒事件	3,105 (29.3%)	跌倒事件	4,595 (28.0%)	藥物事件	7,618 (31.1%)	藥物事件	10,569 (29.0%)	藥物事件	15,569 (31.3%)
2	藥物事件	418 (17.3%)	藥物事件	2,722 (25.7%)	藥物事件	3,845 (23.4%)	跌倒事件	6,462 (26.4%)	跌倒事件	10,094 (27.7%)	跌倒事件	13,581 (27.3%)
3	醫療照護	328 (13.6%)	管路事件	1,130 (10.7%)	管路事件	2,767 (16.9%)	管路事件	3,663 (14.9%)	管路事件	6,138 (16.8%)	管路事件	8,099 (16.3%)
4	傷害行為	244 (10.1%)	傷害行為	1,116 (10.5%)	醫療照護	1,715 (10.4%)	醫療照護	2,038 (8.3%)	傷害行為	2,598 (7.1%)	檢查檢驗	3,323 (6.7%)
5	管路事件	204 (8.5%)	醫療照護	1,005 (9.5%)	傷害行為	1,575 (9.6%)	傷害行為	1,613 (6.6%)	檢查檢驗	2,409 (6.6%)	傷害行為	3,159 (6.4%)
6	其他事件	183 (7.6%)	治安事件	517 (4.9%)	治安事件	766 (4.7%)	治安事件	961 (3.9%)	治安事件	1,517 (4.2%)	治安事件	1,862 (3.7%)
7	治安事件	156 (6.5%)	其他事件	505 (4.8%)	其他事件	335 (2.0%)	檢查檢驗	940 (3.8%)	醫療照護	1,227 (3.4%)	醫療照護	1,543 (3.1%)

圖 1 各年事件類別排行榜(%係指該類事件佔當年度事件數之比例)

其中藥物通報事件數量就有 15,569 件，佔總體的 31.3%。從 2005 到 2010 年統計中，藥物事件自 2007 年以後，就佔通報事件的首位，而且通報數量逐年以平均約六成增長，由此可見藥物事件的嚴重性及威脅國人的醫療安全。在進一步，剖析藥物通報事件，發現病人的就醫類別以住院較多（50.5%），而事件發生可能原因以人為部分為最高(66.1%)，如圖 2。

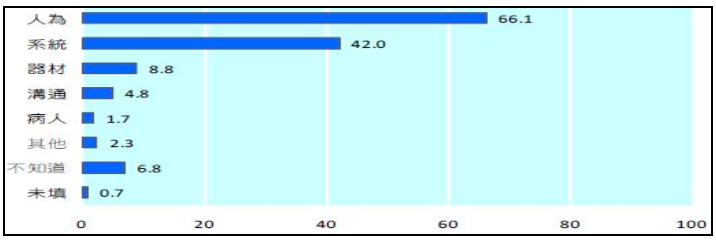

圖 2 醫院藥物事件發生可能原因相對次數百分比

用藥錯誤大致分為處方藥品的錯誤、實施處方單的錯誤、病人接受錯誤的藥物治療、文件錯誤、…等。要減少用藥錯誤，護士在執行配藥行為時必須遵守三讀五對，三讀：取藥時、抽藥時、放回時；五對：病人、藥物、劑量、時間及途徑。醫院使用各種技術來保障他們的用藥行為，如醫師電腦醫令系統(Computerized physician order entry,CPOE)、自動分配系統(Automated Dispensing System,ADS)、條碼系統(Barcode)、無線射頻系統(RFID)等，這些工具是用來防止不同類型的用藥錯誤，如醫囑處方的錯誤、配藥的錯誤、給藥的錯誤等，然而條碼有使用上的諸多限制，如:讀取範圍、資料量、讀取速度與認證安全等，所以在應用趨勢上，會逐漸被 RFID 所取代。

RFID 比條碼在讀取或寫入標籤有更大的範圍、讀取速度與資料容量，而且 RFID 標籤有更好的運算能力，可以做簡單的加解密運算以達認證安全並且可以更新標籤內

之資訊內容。由於 RFID 標籤的這些功能，所以在注重準確性及安全性的醫療系統中，會逐漸廣泛被使用。

在醫療應用方面，RFID引進於醫療資訊系統，可以提高對病人用藥之準確性與安全性並減少醫療錯誤的發生，提供病人一個優良的醫療環境，有效提昇醫療品質與病人安全。Wu[7]提出應用 RFID技術來控管藥物提高病人的用藥安全，Huang[4]提出住院病人用藥安全的RFID群組驗證(Grouping-Proof)協定，但此協定會遭受攻擊(例如重送攻擊、偽造攻擊等)並且對於病人隱私有所疑慮，Pedro[5]提出了一種機制來減少不同類型的用藥錯誤，如處方錯誤，檢驗錯誤，配藥失誤和管理失誤，但此協定尚未提供不可否認性並且會遭受到攻擊。在本論文中，將建立一個安全的RFID雙向驗證機制提供不追蹤性、匿名性、不可否認並抵擋已知攻擊，在護士執行配藥給病人時，能夠達到準確配藥且安全的環境，以減少在配藥上的錯誤，降低發生藥物事故的機率，保障病人的醫療安全。

本論文在第 2 節將介紹目前 RFID 應用在醫療的相關協定，第 3 節介紹本協定的流程，分為初始、登入、驗證階段，第 4 節分析本協定的安全，能抵擋的攻擊以及保障病人的權益並與相關協定做比較，第 5 節提出了結論。

2. 相關研究

在 2009 年 Huang 提出 grouping-proof 協定，利用循環冗餘檢查碼(CRC)和隨機亂數產生方程式(PRNG)等基本運算，他們假設每位病人手腕上有一個附有 RFID 標籤的腕帶，每袋藥或裝藥容器也皆有一個 RFID 標籤，當護士分配藥物時，利用藥物 grouping-proof 協定檢驗藥物是否齊全並確認符合病人的身分，以確保病人的用藥安全。隨後，Chien[2]指出 Huang 協定無法抵抗重送攻擊和拒絕服務攻擊等攻擊行為，而針對 Huang 協定的弱點，提出兩個兩個新的協定。

2.1 Huang 的協定

可以驗證在藥包內的藥物是否與病人所分配的藥物相符。

2.11 符號

Tag i:屬於容器中的第 i 個產品或項目，i=1,2,3,…….,n

Pallet tag:病人腕帶上的標籤

Reader:傳送訊息與產生時間標記

CRC:循環冗餘檢查碼

PRNG:隨機亂數產生方程式

*TS:*時間戳記

EPC_i: Tag i 的 EPC 編號，i=1,2,3,…….,n

PIN_i: Tag i 的識別碼，i=1,2,3,…….,n

EPC_{Pallet}:Pallet tag 的 EPC 編號

PIN_{Pallet}:Pallet tag 的識別碼

2.12 協定，如圖 3 所示。

初始階段

此階段每個 Tag i 會選擇一個隨機亂數 X 作為 PIN_i，i=1,2,3,…….,n，X 為

16 位元的二進制。

溝通階段

讀取機傳送時間戳記 TS 給 Tag_1 與 Pallet tag 並接收 Tag_1 的 EPC_1 與 m_1，對 Tag_2 到 Tag_n 傳送 m_{i-1} 與接收 Tag_i 傳送的 EPC_i 與 m_i，i=2,2,3,…….,n。

驗證階段

讀取機會去驗證 m_i 與 P 是否正確，若正確則去檢查鏈結關係 (EPC_1,…….EPC_n,EPC_{pallet})是否皆為病人的藥物。

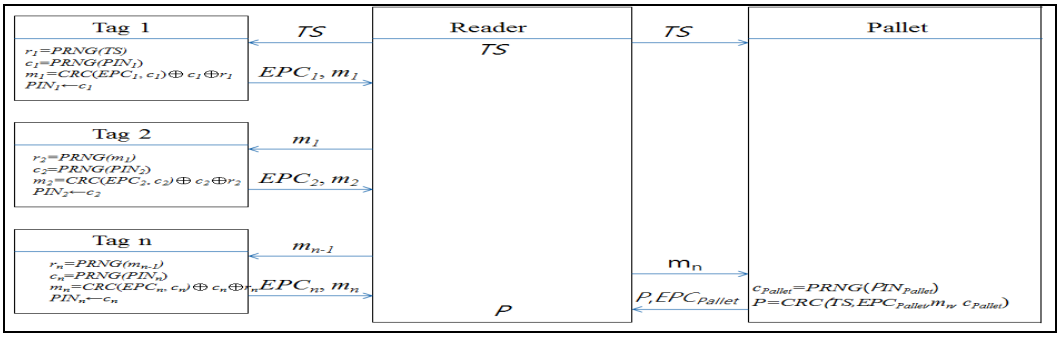

圖 3 Huang 的協定

Chien 的協定

以 OFF-LINE 為例，此協定是基於 Huang 的協定並改善其缺點而成立。

2.21 符號

Tag i:屬於容器中的第 i 個產品或項目，i=1,2,3,…….,n

Pallet tag:病人腕帶上的標籤

Reader:傳送訊息

CRC:循環冗餘檢查碼

$PRNG$:隨機亂數產生方程式

*timestamp:*時間戳記

EPC_i: Tag i 的 EPC 編號，i=1,2,3,…….,n

PIN_i: Tag i 的識別碼，i=1,2,3,…….,n

EPC_{Pallet}:Pallet tag 的 EPC 編號

PIN_{Pallet}:Pallet tag 的識別碼

E:加密演算法

K_V:驗證者的秘鑰

2.22 協定，如圖 4 所示。

一開始讀取機會取得驗證者加密時間戳的訊息 t，讀取機會將加密後的間戳記 t 傳送給 Tag_1 與 Pallet，接下來 Tag i 會計算 m_i 並傳送 EPC_i、m_i，除了 Tag_1 外，每個 Tag i 會收到讀取機所傳送的 m_{i-1}，接下來讀取機會將傳送 m_n 給 Pallet，Pallet 收到讀取機所傳的訊息後，計算相關資訊並傳送 m_{Pallet} 與 EPC_{Pallet} 給讀取機，讀取機會將 (t, EPC_1, m_1, EPC_n, m_n, EPC_{Pallet}, p)傳送給驗證者，驗證者會檢查(EPC_1, ……, EPC_n, EPC_{Pallet})與(m_1, ……, m_n, p)是否皆有在處方籤內，接下來驗證者會去解密時間戳記是否有在可接

受的時間範圍內，如果以上皆達成，則代表驗證成功。i=1, 2, 3, ……, n。

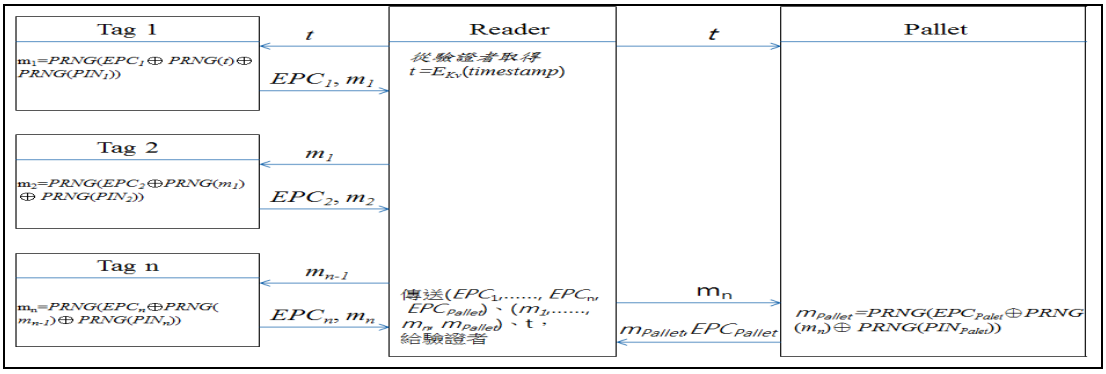

圖 4 Chien 的協定

3. 提出的協定(LIH 協定)

3.1 符號定義

ID_X:某唯一識別身分

PW:護士密碼

X:伺服器祕密值

M_{groupi}:一個只有群組 TAG、讀取機、伺服器才知道的秘密值

M_R:一個只有讀取機跟伺服器知道的秘密值

M_i:一個只有病人標籤、讀取機、伺服器知道的秘密值

M_{nursei}:一個只有伺服器、病人標籤知道的秘密值

$Info$:藥物詳細資訊包含詳細說明、用法、用途、時間、編號

EPCX:tag$_X$ 的 EPC 編號

Key$X$:tag$_X$ 的秘鑰

S_1、S_2、S_3:伺服器、藥劑師、護士的簽章訊息

SSK:使用 RSA 用伺服器私鑰加密

SPK: 使用 RSA 用伺服器公鑰加密

PSK:使用 RSA 用藥劑師私密加密

PPK:使用 RSA 用藥劑師公鑰加密

NSK: 使用 RSA 用護士私鑰加密

NPK: 使用 RSA 用護士公鑰加密

R_{Si}、R_{Ri}、R_P、R_M、r_i、r_j、r_k:伺服器、讀取機、標籤(病人或藥物標籤)產生的隨機數

h():單向雜湊函數

$S_{SSK}(m)$:使用伺服器私鑰簽章訊息 m

$V_{SPK}(m)$: 使用伺服器公鑰驗證訊息 m

$S_{PSK}(m)$: 使用藥劑師私鑰簽章訊息 m

$V_{PPK}(m)$: 使用藥劑師公鑰驗證訊息 m

$S_{NSK}(m)$:使用護士私鑰簽章訊息 m

$V_{NSK}(m)$: 使用護士私鑰驗證訊息 m

⊕:互斥或

+:加法

-:減法

A?=B:決定 A 是否與 B 相同

⟶ :不安全通道

------▸ :安全通道

3.2 初始階段

在初始階段，護士會啟動智慧卡向伺服器註冊，然後伺服器會設置資訊到標籤裡並儲存，然後伺服器會計算驗證相關的訊息並且傳送給智慧卡，讓它可以利用這些驗證資訊去驗證使用者。

首先護士輸入自己的帳號與密碼後啟動智慧卡，智慧卡確認護士為合法的身分後，傳送護士的帳號 ID_{nurse} 與密碼 PW 與隨機亂數 r_i 給讀取機，讀取機經由安全通道傳送護士帳號 ID_{nurse} 與密碼 PW、隨機亂數 r_i 給伺服器註冊，當伺服器收到讀取機的註冊資訊後，會產生隨機亂數 R_{S1} 與整數 q 並利用伺服器秘密值 X 與註冊資訊(ID_{nurse}、PW)去計算 C_1、p、B、B'、W，

$$C_1=ID_{nurse}\oplus h(X||R_{S1}) \quad (1)$$

$$p=2q+1 \quad (2)$$

$$B=[h(ID_{nurse})^x]^{PW-1} \bmod p \quad (3)$$

$$B'=B^{ri}=[h(ID_{nurse})^{x*r_i}]^{PW-1} \bmod p \quad (4)$$

$$W=h(ID_{nurse})^{r_i} \bmod p \quad (5)$$

然後伺服器會計算簽章訊息 S_1:

$$S_1=S_{SSK}(EPC_{patienti})\oplus M_R \quad (6)$$

在自動分配機包完病人的藥物之後，藥劑師會檢查是否藥物與處方簽的內容相同，然後簽署簽章訊息 S_2，

$$S_2=S_{PSK}(EPC_{patienti}、EPC_{medicinei}、info) \quad (7)$$

然後伺服器會設置秘密值 M_i、M_{groupi}、M_{nurse}、EPC 編號 $EPC_{patienti}$、秘密鑰匙 $key_{patienti}$ 與伺服器簽章 S_1 到病人標籤 $T_{patienti}$，伺服器也會傳送秘密值 M_{groupi}、EPC 編號 $EPC_{medicinei}$、秘密鑰匙 $key_{medicinei}$ 與藥劑師簽章 S_2 到藥物標籤 $T_{medicinei}$，最後伺服器經由安全經道傳送 ID_{nurse}、B'、W 到智慧卡儲存，C_1、ID_{nurse} 到讀取機儲存。圖 5 為本協定初始階段流程圖。

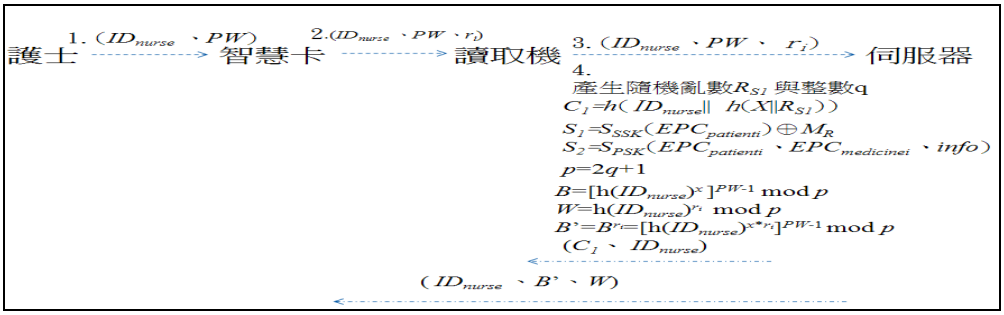

圖 5 初始階段流程圖

3.3 登入階段

在登入階段，護士將輸入帳號與密碼去啟動智慧卡，伺服器驗證護士的身分為合法後，伺服器根據護士的身分獲得配送資訊到讀取機。

一開始護士先輸入帳號 ID_{nurse} 與密碼 PW 到智慧卡，智慧卡收到訊息後，產生隨機亂數 r_j 並計算訊息 B''、R_1、i，經由安全通道傳送給讀取機，讀取機將傳送訊息(ID_{nurse}、B''、R_1、i)給伺服器，

$$B''=B'^{*PW}=\mathrm{h}(ID_{nurse})^{x*ri} \bmod p \quad (8)$$

$$R_1=h(W||B''||ID_{nurse}) \quad (9)$$

$$i=B'\oplus r_j \quad (10)$$

當伺服器收到從讀取機傳送的訊息(ID_{nurse}、B''、R_1、i)後，會去確認護士身分是否合法，

$$B'''=W^x \bmod p \quad (11)$$

$$R_1?=h(W||B'''||ID_{nurse}) \quad (12)$$

若(12)等式相等，則代表護士身分合法，則伺服器會產生隨機亂數 r_k 與計算 h_1，並傳送訊息(h_1、r_k)給智慧卡，

$$r_j'=i\oplus B' \quad (13)$$

$$sk=\mathrm{h}(B'''||r_k||r_j') \quad (14)$$

$$h_1=\mathrm{h}(sk||\ r_k||r_j') \quad (15)$$

當智慧卡收到從伺服器的訊息(h_1、r_k)後，會去確認伺服器是否為合法，

$$sk'=\mathrm{h}(B''||r_k||r_j') \quad (16)$$

$$h_1?=\mathrm{h}(sk'||\ r_k||r_j') \quad (17)$$

若(17)等式相等，則代表伺服器為合法，智慧卡會計算訊息(h_2)並傳給伺服器，

$$h_2=\mathrm{h}(ID_{nurse}||sk') \quad (18)$$

伺服器收到從智慧卡傳送的訊息(h_2)後，會去確認智慧卡的合法性，

$$h_2?=\mathrm{h}(ID_{nurse}||sk) \quad (19)$$

若(19)等式相等，則代表智慧卡為合法，伺服器產生隨機亂數 Rs_2 與配送資訊 $List$，每個組合都包含病人標籤的相關資訊(秘密值 M_i、M_{nurse} 與 M_{groupi}、EPC 編號 $EPC_{patienti}$ 和秘密鑰匙 $key_{patienti}$)和相對應的藥物標籤資訊(EPC 編號 $EPC_{medicinei}$、秘密鑰匙 $key_{medicinei}$ 和資訊 $info$)，

$$List=(EPC_{patient1}、EPC_{medicine1}、M_1、M_{nursei}、M_{group1}、key_{patient1}、key_{medicine1}、info) \quad (20)$$

$$(EPC_{patient2}、EPC_{medicine2}、M_2、M_{nursei}、M_{group2}、key_{patient2}、key_{medicine2}、info)$$

$$(EPC_{patient3}、EPC_{medicine3}、M_3、M_{nursei}、M_{group3}、key_{patient3}、key_{medicine3}、info)$$

然後伺服器會用隨機亂數 Rs_2 並與配送資訊 $List$ 計算訊息(C_2、C_3、C_4)並傳送給讀取機，

$$C_2=h(X||ID_{nurse})\oplus R_{s2} \quad (21)$$

$$C_3=h(ID_{nurse}||\ h(X||R_{s1})||\ R_{s2}) \quad (22)$$

$$C_4=List\oplus R_{s2} \quad (23)$$

當讀取機收到從伺服器傳送的訊息(C_2、C_3、C_4)後，讀取機會利用 C_1 與護士帳號 ID_{nurse} 算出雜湊值 $\mathrm{h}(X||R_{s1})'$，利用雜湊值 $\mathrm{h}(X||R_{s1})'$ 與 C_2 取得隨機亂數 R_{S2}' 並且驗證伺服器是否為合法，

$h(X||R_{s1})' = C_1 \oplus ID_{nurse}$ (24)

$R_{S2}' = C_2 \oplus h(X||R_{s1})'$ (25)

$C_3? = h(ID_{nurse}|| h(X||R_{s1})|| R_{S2}')$ (26)

若(26)等式相等，則代表伺服器為合法，讀取機將利用伺服器的隨機值 R'_{S2} 解密 C_4 去獲得 $List$，

$List = C_4 \oplus R_{S2}'$ (27)

最後，護士依照讀取機中的 $List$ 去執行他/她的工作。圖 6 為本協定登入階段流程圖。

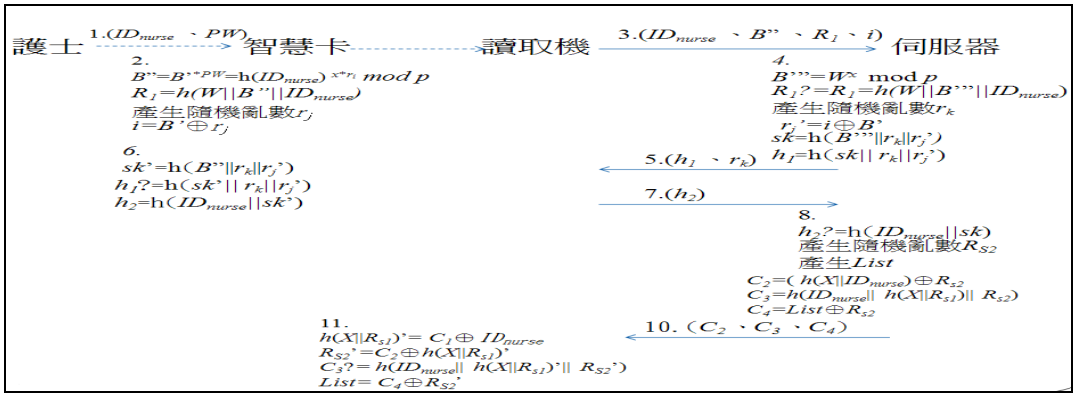

圖 6 登入階段流程圖

3.4 驗證階段

在驗證階段，讀取機發送資訊詢問病人標籤 $T_{patienti}$ 的 EPC 編號 $EPC_{patienti}$，然後去配送資訊 $List$ 找到相對應的藥物資訊，護士會去找尋與此病人標籤 $T_{patienti}$ 為同一群組的藥物標籤 $T_{medicinei}$，這些群組標籤可以經由挑戰與回應來驗證讀取機的合法性，最後護士會將正確的藥物分配給相對應的病人，在分配藥物後護士會用他私鑰簽屬資訊。一開始讀取機會產生隨機亂數 R_{R1} 去詢問病人標籤 $T_{patienti}$ 獲得相關的群組資訊，讀取機會去計算訊息(C_5)傳送給病人標籤 $T_{patienti}$，

$C_5 = R_{R1} \oplus M_{nursei}$ (28)

當病人標籤 $T_{patienti}$ 收到詢問訊息(C_5)後，會用 M_{nursei} 解出隨機亂數 R_{R1}'，

$R_{R1}' = M_{nursei} \oplus C_3$ (29)

然後，病人標籤 $T_{patienti}$ 會利用隨機亂數 R_{R1}' 與秘密值 M_{groupi}，計算訊息(C_6)並且傳送給讀取機，

$C_6 = M_{groupi} \oplus R_{R1}'$ (30)

當讀取機從病人標籤 $T_{patienti}$ 收到訊息(C_6)後，會利用隨機亂數 R_{R1} 與訊息(C_6)解出秘密值 M_{groupi}，觀察配送資訊 $List$，此秘密值 M_{groupi} 是屬於哪位病人並產生隨機亂數 R_{R2}，利用 R_{R2}、病人秘鑰 $key_{patienti}$ 與秘密值 M_{groupi}、M_i 計算訊息(C_7、C_8)並且傳送給病人標籤 $T_{patienti}$，

$C_7 = M_{groupi} \oplus key_{patienti} \oplus R_{R2}$ (31)

$C_8 = key_{patienti} \oplus M_i \oplus R_{R2}$ (32)

當病人標籤 $T_{patienti}$ 從讀取機收到訊息(C_7、C_8)後，會利用秘密值 M_{groupi} 與自身秘鑰 $key_{patienti}$ 取得隨機亂數 R_{R2}' 並且驗證讀取機是否為合法，

$R_{R2}'=M_{groupi}\oplus C_7$ (33)

$C_8?=key_{patienti}\oplus M_i\oplus R_{R2}'$ (34)

若(34)等式相等，則代表讀取機為合法，病人標籤 $T_{patienti}$ 會產生隨機亂數 R_P 去隱藏簽章訊息 S_1 與 EPC 編號 $EPC_{patienti}$，計算訊息(C_9、C_{10}、C_{11})並且傳送給讀取機，

$C_9=R_P\oplus M_{groupi}$ (35)

$C_{10}=S_1\oplus R_P\oplus R_{R2}'$ (36)

$C_{11}=EPC_{patienti}\oplus R_P\oplus M_i$ (37)

當讀取機從病人標籤 $T_{patienti}$ 收到訊息(C_9、C_{10}、C_{11})後，會利用秘密值 M_{groupi} 與 C_9 計算隨機亂數 R_P'，用隨機亂數 R_P'去解密訊息 C_{10} 取得簽章訊息 S_1'，

$R_P'=C_9\oplus M_{groupi}$ (38)

$S_1'=C_{10}\oplus R_P'\oplus R_{R2}$ (39)

然後讀取機會利用伺服器公鑰 SPK、病人標籤 $T_{patienti}$ 的秘密值 M_R、M_i 去驗證伺服器的簽章訊 S_1'，

$(C_{11}\oplus R_{R2}'\oplus R_P')?=V_{SPK}(S_1'\oplus M_R)$ (40)

當驗證完伺服器簽章訊息 S_1'可以得知此病人標籤 $T_{patienti}$ 是不是由合法單位所核發的，若為合法則讀取機會去搜尋配送資訊 $List$ 看有無此病人的 EPC 編號，接下來會獲得病人的藥物標籤 $T_{medicinei}$ 相關資訊，讀取機會產生隨機亂數 R_{R3}，利用 R_{R3}、EPC 編號 $T_{medicinei}$ 和藥物秘鑰 $key_{medicinei}$ 去計算訊息(C_{12}、C_{13})並傳送給藥物標籤 $T_{medicinei}$，

$C_{12}= EPC_{medicinei}\oplus R_{R3}\oplus M_{group}$ (41)

$C_{13}=EPC_{medicinei}\oplus key_{medicinei}\oplus R_{R3}$ (42)

當藥物標籤 $T_{medicinei}$ 從讀取機收到訊息(C_{12}、C_{13})後，藥物標籤 $T_{medicinei}$ 使用它本身的 EPC 編號 $EPC_{medicinei}$ 與 M_{groupi} 解出隨機亂數 R_{R3}'並驗證讀取機的合法性，

$R_{R3}'= C_{12}\oplus EPC_{medicinei}\oplus M_{groupi}$ (43)

$C_{13}?=EPC_{medicinei}\oplus key_{medicinei}\oplus R_{R3}'$ (44)

若(44)等式相等，則代表讀取機為合法，藥物標籤 $T_{medicinei}$ 會產生隨機亂數 R_M，藥物標籤 $T_{medicinei}$ 會使用 R_{R3}'與 R_M 去隱藏藥劑師簽章訊息 S_2 並且使用隨機亂數 R_{R3}'與 R_M、秘鑰 $key_{medicine}$ 去計算訊息(C_{14}、C_{15}、C_{16})並傳送給讀取機，

$C_{14}=EPC_{medicinei}\oplus R_M\oplus M_{groupi}$ (45)

$C_{15}= (S_2\oplus R_M)- (R_{R3}'-1)$ (46)

$C_{16}=(EPC_{medicinei}\oplus key_{medicinei}\oplus\ (R_{R3}'-1)\ \oplus R_M\oplus S_2)$ (47)

當讀取機從藥物標籤 $T_{medicinei}$ 收到訊息(C_{14}、C_{15}、C_{16})後，讀取機會去計算隨機亂數 R_M'並且確認藥物標籤 $T_{medicinei}$ 的合法性，

$R_M'= C_{14}\oplus EPC_{medicinei}\oplus M_{groupi}$ (48)

$S_2'=(C_{15}+ (R_{R3}+1))\oplus R_M'$ (49)

$C_{16}?=EPC_{medicinei}\oplus key_{medicinei}\oplus\ (R'_{R3}+1)\oplus R_M'\oplus S_2'$ (50)

若(49)等式相等，則代表藥物標籤 $T_{medicinei}$ 為合法，讀取機使用藥劑師公鑰 PPK 去驗證 S_2'是否合法:

$(EPC_{patienti}、EPC_{medicinei}、info)?=V_{PPK}(S_2')$ (51)

若(50)等式相等，則代表藥物標籤 $T_{patienti}$ 為合法，接下來護士用他/她的私鑰 NSK 簽屬訊息 S_3 證明護士將藥物分配到正確的病人，

$S_3=S_{NSK}(ID_{nurse}、S_2')$ (52)

最後，讀取機儲存簽章訊息 S_3，當護士與讀取機返回護理站時，讀取機傳送簽章訊息 $(ID_{nurs}、S_2'$與 $S_3)$給伺服器紀錄，抽出智慧卡並初始化讀取機供下一位護士使用。當伺服器收到從讀取機傳送的訊息$(ID_{nurse}、S_2'$與 $S_3)$後，會確認訊息是否正確性，若正確，則儲存。圖 7 為驗證階段流程圖。

$(ID_{nurse}、S_2')?=V_{NPK}(S_3)$ (53)

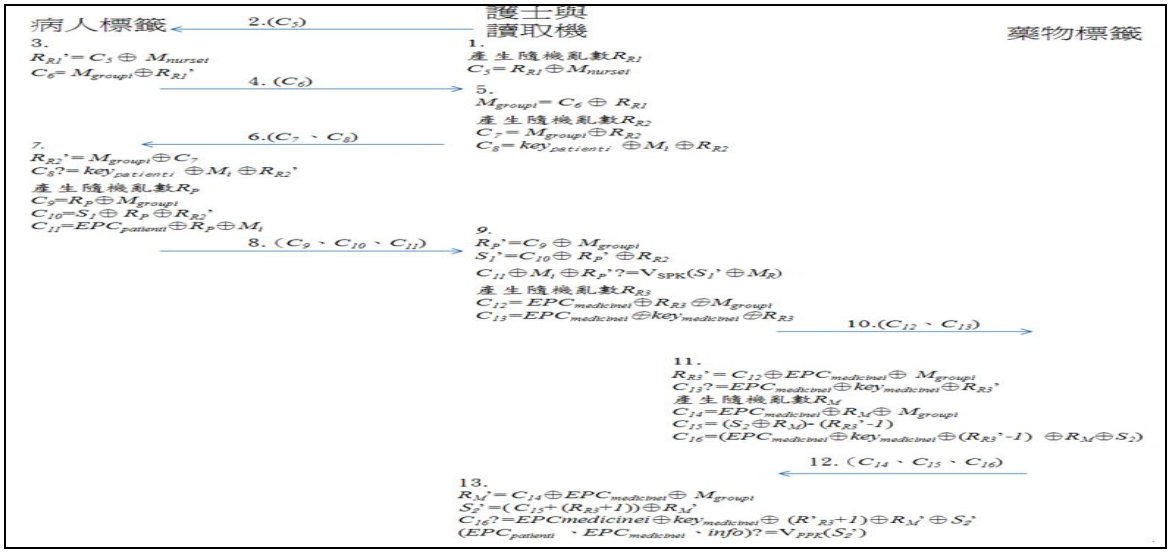

圖 7 驗證階段流程圖

4. 安全分析

4.1 隱私保護

在驗證階段，攻擊者想要獲取病人或是藥物標籤的 EPC 編號，從中攔截病人或是藥物標籤與讀取機溝通的訊息(C_{11}、C_{12}、C_{16})，但由於這些訊息由隨機亂數 R_{R3}、R_P、R_M 與秘密值 M_{groupi}、M_i 加密過，使得攻擊者難以解密進而取得病人或是藥物標籤的 EPC 編號，如此可以保護病人或是藥物標籤的 EPC 編號，以防被攻擊者利用從事不法活動。

$C_{11}=EPC_{patienti}\oplus R_P\oplus M_i$ (37)

$C_{12}= EPC_{medicinei}\oplus R_{R3}\oplus M_{groupi}$ (41)

$C_{16}=(EPC_{medicinei}\oplus key_{medicinei}\oplus\ (R_{R3}'-1)\oplus R_M\oplus S_2)$ (47)

4.2 抵擋重送攻擊

所謂的重送攻擊意指，利用溝通雙方在溝通時傳送的訊息，攔截下來在重送而偽裝成其中一方，讓另一方誤認為攻擊者為合法的一方。在驗證階段，攻擊者可能會攔截到某些由合法方發送的訊息，攻擊者將訊息攔截下來後，再重送訊息給接收方讓接收

方誤認攻擊者就是合法方，進而發送相關訊息給攻擊者或接受攻擊者的請求，在驗證階段，攻擊者攔截到讀取機傳送給病人標籤 $T_{patienti}$ 的訊息(C_5'、C_7'、C_8')與病人標籤 $T_{patienti}$ 傳送給讀取機的訊息(C_9'、C_{10}'、C_{11}')，

$$C_5'=R_{R1}'\oplus M_{nursei} \tag{54}$$

$$C_7'=M_{groupi}\oplus key_{patienti}\oplus R_{R2}' \tag{55}$$

$$C_8'= key_{patienti}\oplus M_i\oplus R_{R2}' \tag{56}$$

$$C_9'=R_P\oplus M_{groupi} \tag{57}$$

$$C_{10}'=S_1\oplus R_P\oplus R_{R2}' \tag{58}$$

$$C_{11}'=EPC_{patienti}\oplus R_P\oplus M_i \tag{59}$$

在下次讀取機要跟同一片病人標籤 $T_{patienti}$ 溝通時，攻擊者重送當初所攔截的訊息(C_5'、C_7'、C_8')給讀取機偽裝病人標籤 $T_{patienti}$，但攻擊者會失敗，原因在於:

$$C_5'=R_{R1}\oplus M_{nursei} \tag{60}$$

$$C_7'=M_{groupi}\oplus key_{patienti}\oplus R_{R2} \tag{61}$$

$$C_8'= key_{patienti}\oplus M_i\oplus R_{R2} \tag{62}$$

當初讀取機所傳送給病人標籤 $T_{patienti}$ 的隨機亂數 R_{R1}、R_{R2} 與假冒的藥物標籤所使用的 R_{R1}'、R_{R2}'不相符，所以讀取機在解密訊息(C_6、C_{10})，會解密失敗與驗證會失敗，代表病人標籤為不合法。

$$M_{groupi}=C_6\oplus R_{R1} \tag{31}$$

$$S_1'=C_{10}\oplus R_P'\oplus R_{R2} \tag{39}$$

另一方面，在驗證階段，攻擊者攔截到讀取機傳送給藥物標籤 $T_{medicinei}$ 的訊息(C_{12}'、C_{13}')與藥物標籤 $T_{medicinei}$ 傳送給讀取機的訊息(C_{14}'、C_{15}'、C_{16}')，

$$C_{12}'= EPC_{medicinei}\oplus R_{R3}'\oplus M_{groupi} \tag{63}$$

$$C_{13}'=EPC_{medicinei}\oplus key_{medicinei}\oplus R_{R3}' \tag{64}$$

$$C_{15}'= (S_2\oplus R_M)- (R_{R3}'-1) \tag{65}$$

$$C_{16}'=(EPC_{medicinei}\oplus key_{medicinei}\oplus (R_{R3}'-1)\oplus R_M\oplus S_2) \tag{66}$$

在下次讀取機要跟同一片藥物標籤 $T_{medicinei}$ 溝通時，攻擊者重送當初所攔截的訊息(C_{14}'、C_{15}'、C_{16}')給讀取機偽裝藥物標籤 $T_{medicinei}$，但攻擊者會失敗，原因在於當初讀取機所傳送給藥物標籤 $T_{medicinei}$ 的 R_{R3} 與假冒的藥物標籤所使用的 R_{R3}'不相符，所以讀取機在驗證訊息 C_{16}，驗證就會失敗，代表此藥物標籤 $T_{medicinei}$ 為不合法。

$$C_{16}?=EPC_{medicinei}\oplus key_{medicinei}\oplus (R'_{R3}+1)\oplus R_M'\oplus S_2' \tag{50}$$

4.3 抵擋中間人攻擊

所謂的中間人攻擊意指，攻擊者在溝通雙方通訊時，攔截一方要傳送過去的資訊，將訊息讀取、更改成自己想要訊息，在發送給另一方，另一方會相信此訊息為合法的或接受攻擊者的要求。在驗證階段，若攻擊者攔截讀取機傳送給藥物標籤 $T_{medicinei}$ 的訊息(C_{12}'、C_{13}')，

$$C_{12}'= EPC_{medicinei}\oplus R_{R3}'\oplus M_{groupi} \tag{67}$$

$$C_{13}'=EPC_{medicinei}\oplus key_{medicinei}\oplus R_{R3}' \tag{68}$$

攻擊者想要偽裝讀取機與藥物標籤 $T_{medicinei}$ 溝通，但由於攻擊者無法得知 EPC 編號

$EPC_{medicinei}$、密鑰 $key_{medicinei}$ 與隨機亂數 M_{groupi}，所以無法更改或是偽造訊息(C_{12}'、C_{13}')。

4.4 不可追蹤性

在驗證階段，病人標籤與讀取機溝通過程中，攻擊者多次攔截到訊息(C_9、C_{10}、C_{11})攻擊者想要得知這些訊息是不是由同一個標籤所發出的，

$$C_9=R_P' \oplus M_{groupi} \tag{36}$$

$$C_{10}=S_1 \oplus R_P' \oplus R_{R2}' \tag{37}$$

$$C_{11}=EPC_{patienti} \oplus R_P' \oplus M_i \tag{38}$$

$$C_9'=R_P' \oplus M_{groupi} \tag{69}$$

$$C_{10}'=S_1 \oplus R_P' \oplus R_{R2}' \tag{70}$$

$$C_{11}'=EPC_{patienti} \oplus R_P' \oplus M_i \tag{71}$$

由於病人標籤 $T_{patienti}$ 每次所產生的 R_P 與讀取機每次產生的 R_{R2} 皆不相同，所以藥物標籤 $T_{medicinei}$ 使用不同的隨機亂數做運算產生訊息的結果也不相同，故攻擊者無法追蹤是不是由同一個標籤所發出的。

在藥物標籤 $T_{medicinei}$ 每次所使用的 M_R 與 R_{R3} 皆不相同，所以產生的訊息結果也不相同，攻擊者也無法藉此追蹤是不是由同一個標籤所發出的。

4.5 相互驗證

在驗證階段中，會利用秘密值或是隨機亂數作挑戰與回應，來驗證標籤或是讀取機的合法性，在讀取機與病人標籤溝通中，讀取機利用 M_{groupi} 與隨機亂數 R_{R1} 計算訊息(C_5)傳給病人標籤 $T_{patienti}$，

$$C_5= R_{R1} \oplus M_{nursei} \tag{28}$$

病人標籤利用秘密值 M_{nursei} 來確認讀取機是不是合法的，病人標籤會利用 R_{R1}'去計算訊息(C_6)並傳送給讀取機

$$C_6=M_{groupi} \oplus R_{R1}' \tag{30}$$

讀取機會用當初所傳送的 R_{R1} 去驗證訊息(C_6)來確認病人標籤 $T_{patienti}$ 的合法性。在讀取機傳送訊息(C_{12}、C_{13})給藥物標籤 $T_{medicinei}$，

$$C_{12}= EPC_{medicinei} \oplus R_{R3} \oplus M_{groupi} \tag{41}$$

$$C_{13}=EPC_{medicinei} \oplus key_{medicinei} \oplus R_{R3} \tag{42}$$

藥物標籤 $T_{medicinei}$ 收到後會利用 EPC 編號 $EPC_{medicinei}$ 與秘密值 M_{groupi} 來解密隨機亂數 R_{R3} 並利用訊息(C_{13})來驗證讀取機的合法性，

$$C_{13}?=EPC_{medicinei} \oplus key_{medicinei} \oplus R_{R3}' \tag{44}$$

接下來藥物標籤會利用 R_{R3}'計算訊息(C_{14}、C_{15}、C_{16})傳送給讀取機，

$$C_{14}=EPC_{medicinei} \oplus R_M \oplus M_{groupi} \tag{45}$$

$$C_{15}= (S_2 \oplus R_M)-(R_{R3}'-1) \tag{46}$$

$$C_{16}=(EPC_{medicinei} \oplus key_{medicinei} \oplus (R_{R3}'-1) \oplus R_M \oplus S_2) \tag{47}$$

讀取機會利用當初所傳送的 R_{R3}'去檢驗訊息(C_{16})來確認藥物標籤 $T_{medicinei}$ 的合法性。

$$C_{16}?=EPC_{medicinei} \oplus key_{medicinei} \oplus (R'_{R3}+1) \oplus R_M' \oplus S_2' \tag{50}$$

4.6 不可否認性

在藥劑師確認自動分配機所打包的藥物與處方簽相同時，藥劑師就會利用他/她的

私鑰 PPK 簽章訊息 S_2 並傳送給伺服器，代表此藥物是經由此藥劑師確認過的，伺服器收到後會確認訊息並紀錄，所以藥劑師無法對經手的藥物否認。

$$(EPC_{patienti}、EPC_{medicinei}、info)?=V_{PPK}(S_2) \quad (72)$$

當護士執行完配藥的任務以後，護士會利用他的私鑰 NSK 簽屬簽章訊息 S_3，讀取機會儲存護士的簽章訊息，當護士返回護理站時，讀取機會傳送護士簽章給伺服器，伺服器收到後會確認訊息並紀錄，所以護士無法對所執行的配藥任務否認。

$$S_3=S_{NSK}(ID_{nurse}、S_2') \quad (52)$$

4.7 匿名性

我們利用隨機亂數 R_S、R_{Ri}、R_P、R_M、R_{R3} 與密鑰 $key_{medicinei}$、$key_{patienti}$ 去加密病人與藥物的 EPC 編號，若攻擊者要破解訊息內容而得知病人與藥物的 EPC 編號，將會無法破解，因為攻擊者不知道隨機亂數與密鑰，所以對於 EPC 編號有達到匿名性。

4.8 相關協定比較

我們比較了相關的協定，如表 1，本論文的協定可以抵擋其他協定會遭受的攻擊，在 Huang 與 Chien 攻擊者可以攔截標籤所傳送的訊息，更改訊息內容使自己能偽裝成合法的標籤，並且由於標籤在傳送給讀取機的訊息中，EPC 編碼 EPC_i 是採用明文傳輸，所以攻擊者可以追蹤是不是由同一個標籤所發出的訊息，讀取機在傳送訊息給標籤並未驗證標籤的合法性，所以訊息接收方可能為攻擊者，在病人取得藥物後，無法得知當初是由哪個藥劑師所核發的或哪位護士分配的，若是往後發生問題難以究責。在我們的協定中，利用隨機亂數與秘鑰加密訊息，把 EPC 編碼利用演算法隱匿起來，使攻擊者無法追蹤訊息，並利用挑戰與回應來驗證雙方得合法性，護士與藥劑師在分配完藥物後都必須簽屬簽章訊息，藉此可以保護病人的權利。

表 1 各協定比較表

協定 / 攻擊方法	Huang	Chien	本論文
抵擋重送攻擊	No	Yes	Yes
抵擋中間人攻擊	No	No	Yes
不可追蹤性	No	No	Yes
相互認證	No	No	Yes
匿名性	No	No	Yes
不可否認性(藥物)	No	No	Yes

5. 結論

在過去幾年的醫療事件中，藥物疏失事件位居事件之首[8]，其中藥物事件的發生又以人為居多，隨著醫療技術的進步，藥品的種類逐漸增加，相似的藥名與包裝容易造成藥劑師分辨上的錯誤，護理人員分配藥物時給病人也容易誤認，用藥與配藥的準確性攸關病人的醫療安全，是不得容緩的重要議題。在本論文中，我們提出一個安全的 RFID 驗證機制，核對病人與藥物交由標籤與讀卡機來執行，讀卡機進行核對標籤正

確後在由護士配送藥物給病人，如此可降低人工作業的疏失，標籤與讀取機的相互認證來防止非法的行為介入，提供匿名性與不可追蹤性來保護病人的隱私權，以避免病人的隱私被非法人員的侵犯，對於病人的藥物，護士與藥劑師皆具有不可否認的責任，如此可以保障病人的權益，提升病人的醫療品質。

參考文獻

[1] Chen,C.L.,Wu,C.Y.,UsingRFID Yoking Proof Protocol to Enhance Inpatient Medication Safety, Journal of Medical Systems.,2011.DOI:10.1007/s10916-011-9763-5

[2] Chien, H.-Y., Yang, C.-C., Wu, T.-C., and Lee, C.-F., TwoRFID-based solutions to enhance inpatient medication safety, Journal of Medical Systems.,2009.DOI:10.1007/s10916-009-9373-7.

[3] Hickner, J., Zafar, A., Kuo, G.M. et al.,Field test results of a new ambulatory care medication error and adverse drug event reporting system-MEADERS, Annals of Family Medicine.,pp.517-525, 2010.

[4] Huang,H.H. and Ku,C.Y.,A RFID grouping proof protocol for medication safety Of inpatient.,Journal of Medical Systems. 33(6), pp.467–474, 2009.

[5] Pedro, P-L., Agustin, O., Aikaterini, M., and Jan, C.A.V. L., A comprehensive RFID solution to enhance inpatient medication safety, International Journal of MedicalInformatics. 80(1), pp. 13–24, 2011.

[6] Sun,P.R.,Wang,B.F. and Wu,F.,A new method to guard inpatient medication safety by the implementation of RFID, International Journal of Medical Informatics. DOI: 10.1007/s10916-008-9137-9

[7] Wu, F.,Kuo,F.,andLiu, L.W., The application of RFID on drug safety of inpatient nursing healthcare, the 7th International Conference on Electronic Commerce., 2005.pp. 85–92

[8] 行政院衛生署，2011，台灣病人安全通報系統2010年年報。