**FEE: 以快速健康照護互操作性資源(FHIR)及以太坊(ETH)智能合約完成具資料完整性的電子病歷資料庫(EMR)**

**(Ensuring Data Integrity in Electronic Medical Records by FHIR and ETH Smart Contracts)**

**楊慶隆 李佾 陳祁鎔 周宗翔 郭新拳**

**國立東華大學資訊工程學系**

**E-mail: cnyang@gms.ndhu.edu.tw**

摘要

依據全球資料庫網站Numbeo的調查，台灣在醫療保健指數評比排行均在前三、且多次奪冠。若現有醫療機構能有互通資料的標準、就能更進一步的將多方數據、異質性設備、新技術整合，讓台灣健保制度更發揮其實質化功效、讓更多人受益。近來，愈來愈多國家的醫療機構，開始採用HL7最新的醫療資料交換標準 "快速健康照護互操作性資源" (FHIR; Fast Healthcare Interoperability Resources)，來做資料的互通。這些資料涵蓋的範圍很全面，不只有醫療機構也包括保險機構、以及相關醫療資訊服務業者。FHIR並未強制要求採用單一技術方案來保護安全和隱私，因此本文使用FHIR並結合以太坊(ETH) 區塊鏈建置、實作一個具資料完整性的電子病歷資料庫 (EMR; Electronic Medical Records)，簡稱FEE。在我們的FEE機制，使用者在登入系統前端頁面時，會透過智能合約採用NFT憑證的方法完成認證。之後，才可執行後端資料庫的運算。登入紀錄、與認證結果皆會記錄在區塊鏈，使得惡意冒名的登入都可追溯。另外，為達到資料完整性，上傳至EMR資料庫的病歷計算後的雜湊值也會上傳至區塊鏈。每當資料庫病歷的內容經過合法更動後便會修改存於區塊鏈。因為病歷版本與雜湊值皆存於區塊鏈，所以可達到資料完整性避免病歷遭到造假及非法使用。

**關鍵詞**：區塊鏈、以太坊、智能合約、FHIR、非同質化代幣NFT、電子病歷EMR。

Abstract

According to a survey by Numbeo, the world’s largest database of user contributed data about cities and countries, the ranking of the health care index for Taiwan is always in the top three and has won the championship for many times. If there is an interoperability standard for electronic medical records (EMR), we can further integrate heterogeneous equipment and new technologies, such that that Taiwan health insurance can play its substantial role and benefit more people. Recently, more countries adopt the latest standard "fast healthcare interoperability resources" (FHIR) for medical data exchange. All these data cover a very comprehensive range, including not only medical institutions but also insurance institutions and related medical information service providers. In fact, FHIR does not mandate using a single solution for security and privacy. In this work, we use FHIR and ETH Smart Contracts to ensure data Integrity in EMR (referred to as FEE). When users log in FEE, they are verified first based on NFT certificate by using Ethereum (ETH). After verification, they may access the EMR data base. All the login records and authentication results are stored on the blockchain, and thus malicious logins can be backward traced. In addition, to ensure data integrity, the hash computation of EMR data is also uploaded to the blockchain. Whenever the content of the medical records in EMR database is legally modified (or updated), the new hash values will be stored in blockchain. Because both the version of medical record and the hash value are stored on blockchain, data integrity can be achieved to prevent medical records from being maliciously used.

**Keywords**：Blockchain, Ethereum, Smart contract, FHIR, NFT, EMR.

1. 前言

一般而言，患者有時會在不同醫療院所接受診斷及治療。若醫療資訊沒有統一格式，就無法快速有效地交換、整合不同醫院的電子病歷以達到跨院診療的需求。不同院所間醫療資訊的交換、及互通性能可以大幅提升全民醫療體系的完整性。以現在新冠肺炎疫情期間的視訊診療為例，負責診療的醫院若需要高風險病人在其他醫療機構的電子病歷，具有互通的醫療資料交換標準在電子資料交換標準資料的使用、傳輸、共享就有利於視訊診療。

全球專門制定醫療資料交換的國際標準組織HL7 [1] 2005年推出的HL7 CDA R2是台灣現用的醫療資訊交換標準，但是它缺乏統一的資料規範、不易支援行動裝置已逐漸被淘汰。因此，衛福部正推廣使用HL7新制定的"快速健康照護互操作性資源" (FHIR; Fast Healthcare Interoperability Resources) 標準來取代舊有的標準。FHIR的固定病例格式解決缺乏統一規範的問題，病歷可在不同醫療院所中傳遞並使用。FHIR也使用了表現層狀態轉移 API (RESTful API; Representational State Transfer API) ，使資料可在行動裝置中傳遞與AIoT結合，運用更加多元。此外，FHIR標準很有彈性，可適應任何相關使用者的需求、臨床醫療的規範、和各別國家的健保政策。

綜合上述優點，愈來愈多國家都已開始使用FHIR標準、並開發相關的套件。FHIR並未強制要求採用單一技術方案來保護安全和隱私。例如，參考文件 [2]，提出SecFHIR的介面模組功能來提高FHIR安全性。雖然FHIR沒明確的認證規範，但在官方文件中建議使用OAuth 作為身分認證標準 [3]。FHIR目前已廣泛應用於實現患者醫療、健康記錄的操作互通性上[4, 5]。有些研究更結合了FHIR與區塊鏈 [6, 7]，以達到更安全地使用FHIR。本文也是，我們使用FHIR及以太坊(ETH)智能合約來建置、實作一個具資料完整性的電子病歷資料庫 (EMR; Electronic Medical Records)。我們的系統簡稱FEE，可提供使用者基於NFT憑證的身分認證、並確保電子病歷的資料完整性。本文結構如下，第二部分為文獻探討，介紹電子病歷EMR、FHIR、以太坊、及RESTful API。第三部分為FEE系統研究動機與設計概念，第四部分則為實作的過程，最後為結論。

1. **文獻探討**
   1. **電子病歷EMR**

電子病歷EMR是將傳統的紙本病歷電子化。易於儲存，有著傳統病歷所沒有的優點，更易於查詢、管理、及適用於不同醫療院所間的互通性操作。電子病歷內容可包含診療紀錄、藥物過敏史、各項檢查報告、及疫苗施打紀錄等。電子病歷的發展對於醫療照護的進步、及不同院所間病歷的交換十分重要。它能有效地降低醫療成本及加速診療流程，讓醫院及病患兩方都有更完善、有效的醫療體驗。總結來說，電子病歷提高對病患的診斷、治療品質，也可以減少醫療差錯。

* 1. **FHIR**

FHIR透過統一資料格式，可於不同醫療院所中相互傳輸、匯出、調閱醫療資料。患者至不同醫院就診，就不需要建置新病例造成資源的浪費。FHIR也支援臨床、非臨床資料，並可於不同裝置及平台中互通，解決不同醫材、不同廠商、不同資料格式的互操作的應用困難。舊的CDA R2僅可支援XML格式，而FHIR可同時支援XML及JSON [8]。JSON的檔案格式較XML在儲存空間及傳輸上有優勢。FHIR有大量的社群提供輔助工具，資料可以進一步的分析。建置FHIR是以一系列資源物件組成，故使用者可以輕易使用、微調這些資源物件，因此我們可。以快速實做臨床醫療實務的應用為例，這些資源物件就是由病患的各項資料組成，如身份證字號、姓名、看診紀錄、檢驗報告等。此外， FHIR支援行動應用資料交換的互通架構，可在各種行動裝置上傳輸資料，如手機、Kiosk、以及AIoT醫療設備，能有效解決CDA R2的侷限應用。在檔案傳輸方式上，台灣電子病歷交換中心以自行開發的專用API，以閘道器擷取、傳輸CDA R2格式資料。FHIR則採用網頁應用，以及行動APP常使用的RESTful API做為資料串接的方式。所以FHIR能適用於更多網頁應用的方式。

* 1. **以太坊 ETH**

區塊鏈是一個去中心化、權限分散式的機制，可以在網絡節點之間複製和分享，而不依賴第三方。通過分散式節點，執行網路數據驗證和儲存的一種去中心化資料庫。它的每個區塊記錄並存儲了某段時間內的交易數據，且每區塊包含了前一區塊的雜湊值。所有雜湊值鏈接一起形成區塊鏈。區塊鏈由眾多礦工維護，採用 "工作量證明" (PoW; Proof of Work) 作為共識機制。PoW代表透過大量算力找出隨機調整數來決定下個區塊的添加者，並給予以太坊的原生代幣以太幣作為獎勵，該代幣可作為鏈上Gas消耗或是其他用途，這個過程就是所謂的 "挖礦"。另外一種共識機制是Proof of Stake (PoS )，它是透過質押的數量及時間作為區塊添加者的依據，透過這個方式解決算力造成的能源消耗並保留去中心化的功能。網絡的每個節點都能查看公開區塊鏈的信息。

除非同時駭入、破壞51%的節點，否則無法對區塊鏈完成51%攻擊。與傳統集中式資料庫相比，區塊鏈可抵抗竄改、節點容錯、不需第三方認證機構的節點間互信的協作能力、允許任何節點獲取整個區塊鏈。

以太坊是一種區塊鏈技術 [9]，是佈放於計算機網路運行可以驗證區塊及交易的程式，該佈放式計算機網路也被稱為節點。以太坊的運作節點存在以太坊虛擬機(EVM; ETH Virtual Machine)，在固定環境中執行被編譯為EVM Bytecode的智能合約。智能合約則是一種運行在區塊鏈上的程式，並且需要先編譯成EVM可以判別的Bytecode後才能部署上區塊鏈執行。並且EVM中的Opcode有相對應的價格，執行智能合約時會消耗相應價格的以太幣 [10]，用來防止惡意的鏈上資源消耗。智能合約也同時有上鏈後無法更改、公開透明等特點，因此常被用作去中心化需求的開發。一般的網路服務在部署後仍需要維持伺服器的運作才能確保服務的運行，但區塊鏈上的智能合約僅需於部署時支付費用即可儲存於以太坊的節點中，並且僅在需要對鏈上資料作更新時才需要再次支付Gas。部署上鏈後，智能合約透過ABI (ABI; Application Binary Interface) 與其他程式或合約進行互動 [11]。ABI描述了合約中函式的使用方式，包括修飾詞、函式名稱、參數、回傳值等。ABI以JSON格式儲存，進行特殊的編碼轉變為EVM可以理解的Bytecode格式後進行互動。

* 1. **RESTful API**

與自訂的API比較，RESTful API 有較佳的資料存取效益。RESTful API [12] 能讓兩個電腦系統安全地透過網際網路交換資訊介面，RESTful API為一種軟體架構，對於API的運作方式施加了條件，可以輕鬆實作和修改，提供可視性及跨平台移植性。RESTful API是REST架構的Web服務，而Web API可被視為用戶端及Web上資源間的通道。由於RESTful API具有可擴展性、靈活性及獨立性的優勢。RESTful API的基本功能和網際網路相同，用戶端使用API聯絡伺服器，而RESTful API請求包含唯一資源識別符 (伺服器通常使用URL進行資源識別)及方法 (通常使用HTTP實作RESTful API)，四種常見對資源做的HTTP方法為：GET (用於存取伺服器上指定URL的資源)、POST (用於向伺服器傳送資料)、PUT (用於更新伺服器上的現有資源)、DELETE (用於請求移除資源)。圖1是使用Swagger自動建立REST API文件的範例。

一張含有 文字 的圖片

自動產生的描述

**圖 1. HAPI FHIR範例**

1. **FEE系統: 植基於FHIR與ETH具資料完整性的EMR** 
   1. **FEE系統研究動機**

因應新冠肺炎疫情，愈來愈多醫院參與了視訊診療指定院所來完成遠距診斷及索取處方籤，所以電子病歷已被廣為使用。台灣目前仍使用操作互通性不高及無統一格式的CDA R2標準。為了降低當前臺灣醫療院所間傳輸資料的成本以及提升操作互通性，故本研究欲引用具有統一格式的FHIR作為電子病歷之標準。因為FHIR標準已被許多國家所採用為醫療資訊交換標準，對於開發者來說也有相當多的開源輔助套件以協助分析資料。但是，FHIR標準並未提供電子病歷安全上的規範，所以我們擬結合FHIR標準與區塊鏈技術，實作一個具有安全認證及電子病歷完整性系統。

* 1. **FEE系統設計概念**

FEE系統開發設計過程，我們會使用Hardhat作為智能合約開的框架，幫助智能合約開發、測試及上鏈，並使用Alchemy作為RPC server與鏈上合約互動與調用。在FHIR資料庫中使用JSON格式取代常規的XML格式，獲取更好的儲存、傳輸效率。最後結合前端Angular框架構建前端頁面，讓使用者可以清楚簡易地操作FHIR中的API對資料進行調閱或是修改。

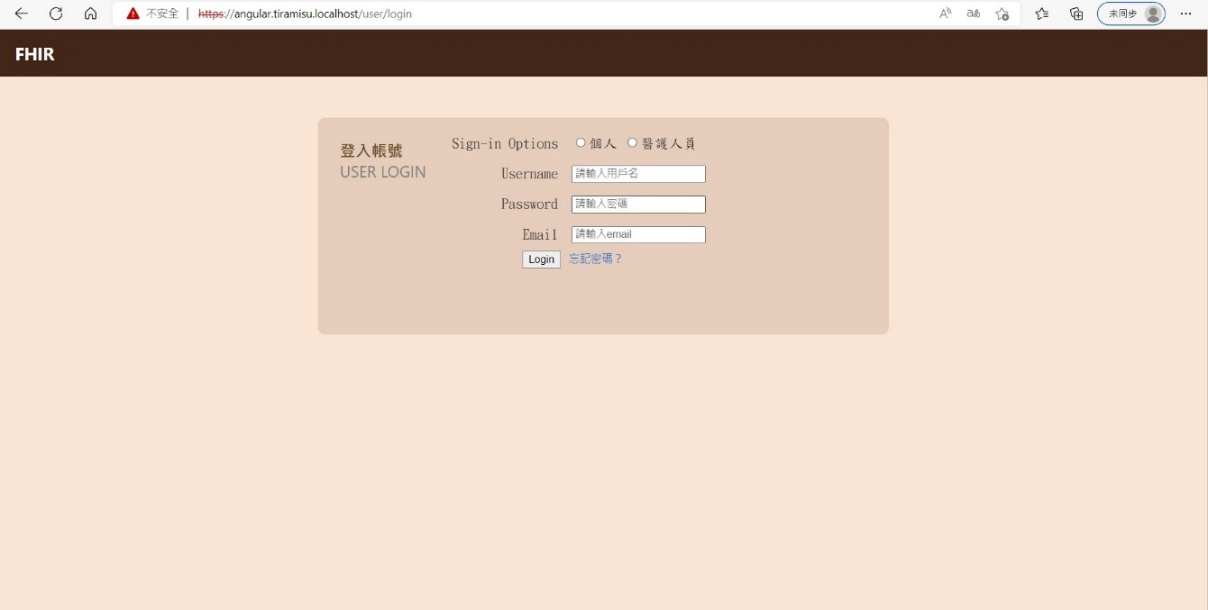
我們的FEE系統提供使用者身分認證、並確保電子病歷的資料完整性。使用者在登入系統前端頁面時，會先呼叫智能合約進行身分驗證，才可呼叫後端操作資料庫。登入紀錄還有驗證結果皆會記錄在區塊鏈，使得惡意冒名的登入都可追溯。我們FEE系統的使用者認證方式參考了NFT證書的實作方式 [13]，將使用者的錢包地址(公鑰)簽章，此簽章可以作為註冊有效的證書使用，使用者提供身分認證證書供資料庫平台檢查，證書與使用者的錢包綁定，使得第三者難以冒用、複製，因使用者的錢包資訊(密碼)只會自己擁有而不會記錄在資料庫內。此步驟避免了使用者帳號密碼洩漏導致冒名登入的安全問題，冒名者無法順利通過身分驗證合約，因簽章地址與冒名者的地址並不一致。

另外，為了達到資料完整性，平台所上傳的病歷會先為每筆報告/病例，計算其雜湊值後上傳至區塊鏈。當資料庫病歷的內容合法更動後，便會修改原本儲存的雜湊值。因為病歷版本及每次計算的新計算其雜湊值皆會紀錄在區塊鏈，只要報告/病例內容或例雜湊值遭到非法更動，便可得知此資料已遭到竄改。

總結而言，本文所提之FHIR系統配合智能合約共分兩大部分。第一部分，使用者進行操作資料庫時，會先需要進行智能合約的身分驗證，用者帳號(錢包地址)均紀錄於區塊鏈上，透過檢查登入使用者的錢包地址是否也在區塊鏈上來達到權限控管。第二部分則是資料完整性，每個病人的病歷皆為一雜湊樹(Merkle tree)。電子病歷更改或新增後，皆會增加或修改樹的節點，而在進行新增或修改前，會先驗證電子病歷資料的雜湊值是否與Merkle root一致，確保資料的完整性。

1. **FEE系統實作**
   1. **前、後端部署**

由於Angular是Single Page Applications (SPA)，我們需使用routing的方式連接各個頁面，SPA能有效提高發布效率、節省原生開發成本及符合Web2.0的趨勢之優點。圖2為完成的使用者登入頁面，含個人及醫護人員。我們初步擬完成個人認證，讓病患下載個人檢驗報告。另外，醫護人員的認證則是讓醫生登錄後，可以修訂、上傳、下載電子病歷，圖3是醫生填寫電子病例的頁面。



**圖 2. 登入系統**



**圖 3. 填寫病例系統**

圖4為預設導向至user module之route，圖5為導向至user module內的登入頁面或病歷填寫系統之route，而我們預設首頁即為登入頁面，故routing方式會先至user module再進到user module內的登入頁面。圖6的submit function會於按下login時被呼叫並導向填寫病例之頁面。

**一張含有 文字 的圖片

自動產生的描述**

**圖4. 預設routing至user module之程式碼**

****

**圖5. user module至登入或填寫病例之route**

**一張含有 文字 的圖片

自動產生的描述**

**圖6. 以submit function實做頁面跳轉**

操作前端介面輸入資料後, 按下操作的按鈕會觸發圖7的addRecord函式。將網頁表單中的病歷資料轉為JSON的字串格式，再透過POST API將資料傳送至後端伺服器。圖7為上傳資料API操作之程式碼。後端伺服器收到API請求後，依據GET/POST/PATCH/PUT/DELETE標頭觸發相對應的函式。在確認資料及權限無誤後，與資料庫進行交互請求，最終回傳執行結果給前端。



**圖7. 上傳資料之API操作**

圖8~圖12為各個標頭檔觸發的相對應函式。透過API將伺服器資料回傳後，將欲呈現資料的欄位定位，並符合typescript規則將資料型態轉為HttpInputElement後將值填入。圖13則為獲取資料API操作之程式碼。

一張含有 文字 的圖片

自動產生的描述

**圖8. GET API所觸發之函式**

**一張含有 文字 的圖片

自動產生的描述**

**圖9. POST API所觸發之函式**

**一張含有 文字 的圖片

自動產生的描述**

**圖10. PATCH API所觸發之函式**

**一張含有 桌 的圖片

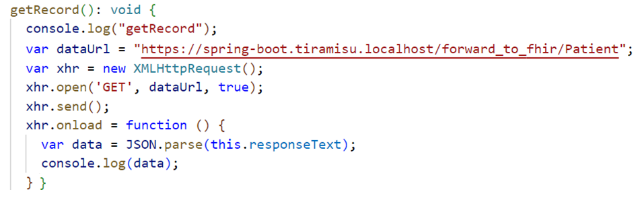
自動產生的描述**

**圖11. PUT API所觸發之函式**

一張含有 文字 的圖片

自動產生的描述

**圖12. DELETE API所觸發之函式**

****

**圖13. 獲取資料之API操作**

* 1. **智能合約**

為求達到資料庫完整性無虞，避免在檔案或檢驗報告因為易於互通交換等特性，使得檔案遭到非預期的修改，我們會需要可信賴的第三方去驗證我們的資料內容是否與原本檔案一致，然後在此條件下，我們必須完全信任第三方稽核，這樣可能會有第三方稽核與資料庫系統的廠商有密謀之虞，使得用戶無法完全信賴，特別是針對個人極其敏感的醫療相關資訊，在此我們提出了使用智能合約(Smart Contract)，作為我們資料庫檔案的審計員，因其去中心化特性，操作皆會記錄在區塊鏈上，且合約內容是公開透明的，所有用戶都能檢閱，這樣我們不再需要依賴可信賴的第三方。圖14是我們FEE系統的資料交互概要示意圖。



**圖 14. FEE系統資料交互概要示意圖**

圖14包括了身分註冊、認證階段、資料庫操作階段、和資料庫認證階段。詳細說明如下:

【**階段1**】**身分註冊、認證階段:**

**(步驟 1-1)**

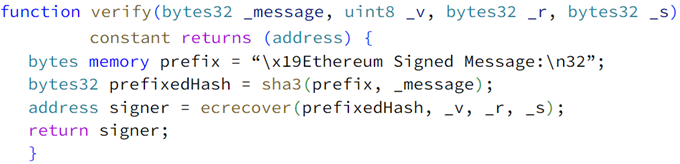
使用者在註冊步驟時，傳送註冊請求給身分認證智能合約，智能合約記錄使用者錢包地址，帳號名稱、及相關訊息。身分認證智能合約發布者(即管理者)，根據使用者註冊資料，進行權限分配。例如，醫生可以製作、修改、查看電子病歷以及病患相關檢查報告。一般使用者(病患)只能查看自己的檢驗報告。管理者分別為不同的權限、屬性建立不同的存取控制，對其錢包地址使用簽章 (圖15) 並回傳給用戶。



**圖15. 簽章合約程式碼**

**(步驟 1-2)**

使用者在認證步驟呼叫認證智能合約時，智能合約會根據solidity ecrecover函數計算得到簽名者的公鑰(即簽名者錢包地址)，檢查地址是否為管理者錢包地址，及被簽名的地址是否為呼叫合約的使用者，以此來達到身分認證。ecrecover簽章解回的智能合約程式碼如圖16所示。



**圖16. ecrecover簽章解回合約程式碼**

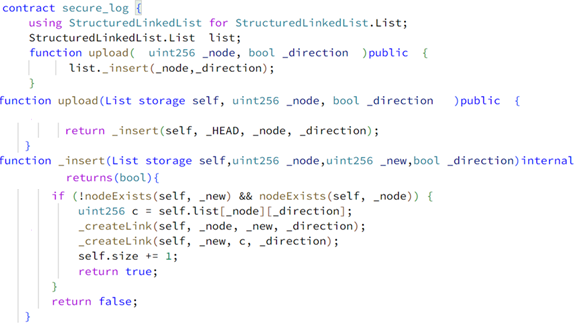
**(步驟 1-3)**

經過 (步驟 1-2) 智能合約完成認證後，決定使用者是否有權限至相關資料庫操作。

【**階段2**】**資料庫操作階段:**

**(步驟2-1)**

使用者在前端頁面依照自己的權限做資料庫的相關處理，然後進行雜湊運算。雜湊值與(步驟1-1) 的身分認證簽章，發送給資料完整性智能合約。合約驗證身分正確後，將雜湊值上傳到區塊鏈上。圖17是為每筆雜湊新增一個節點編號儲存雜湊值，使用雙向鏈結串列的方式儲存，避免因節點刪除，而遺失刪除節點後的串列。



**圖17. 簽章合約程式碼**

**(步驟 2-2)**

FHIR資料庫接受、並儲存來自前端頁面所新增或修訂的資料。

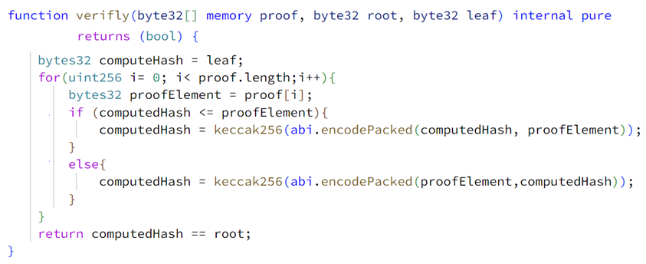
【**階段3**】**資料庫認證階段:**

**(步驟3-1)**

當醫生需要查看病歷(或一般使用者查看檢驗報告時)，先傳送驗證請求到FHIR資料庫。讀取資料後，進行雜湊運算以得其Merkle root。將結果與資料回傳至完整性智能合約做驗證。

**(步驟 3-2)**

合約(圖18)接受到驗證請求以及RootFHIR ，依據節點編號，建立Merke root，並比對認證結果RootFHIR與RootBlockChain是否一致，將結果回傳。



**圖18. 計算與認證Merkle root合約程式碼**

1. **結論**

若醫院無醫療資料互通標準，就無法達到跨醫療院所的醫療資料交換、與快速整合。HL7的最新標準FHIR協議已逐漸成為醫療資料互通的世界標準。另外，由於FHIR並未強制要求採用單一技術方案來保護安全和隱私。本文使用FHIR並結合以太坊區塊鏈建置、實作一個具資料完整性的電子病歷資料庫FEE。我們的FEE安全機制包含使用者驗證、及電子病歷資料庫的完整性。

1. **參考文獻**
2. HL7國際組織: https://www.hl7.org/.
3. A.M. Altamimi, “SecFHIR: A Security Specification Model for Fast Healthcare Interoperability Resources,” I*nternational Journal of Advanced Computer Science and Applications*, Vol. 7, pp. 350-355, 2016.
4. FHIR安全認證建議: https://www.hl7.org/fhir/security.html# authentication.
5. R. Saripalle, C. Runyan, and M. Russell, “Using HL7 FHIR to Achieve Interoperability in Patient Health Record,” *Journal of Biomedical Informatics*, Vol. 94, Article 103188, 2019.
6. 俞國靖等, "符合快速健康照護互通資源標準的數據集製作與管理",國際醫學資訊聯合研討會, 九月, 2021.
7. H. Kung, Y. Cheng, H. Lee, and C. Hsu, “Personal Health Record in FHIR Format Based on Blockchain Architecture”, *International Conference on Frontier Computing*, LNEE Vol. 551, pp. 1776-1788, 2019.
8. A. R. Lee, M. G. Kim and I. K. Kim, "SHAREChain: Healthcare Data Sharing Framework Using Blockchain-registry and FHIR," 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), pp. 1087-1090, 2019.
9. FHIR 檔案範本: https://hl7.org/fhir/patient-example.html.
10. 以太坊開發文件: https://ethereum.org/zh-tw/developers/docs/.
11. Ethereum區塊鏈！智能合約(Smart Contract)與分散式網頁應用(dApp)入門: https://gasolin.gitbooks.io/learn-ethereum-dapp/content/.
12. What is an ABI of a Smart Contract?: https://www.alchemy. com/overviews/what-is-an-abi-of-a-smart-contract-examples-and-usage.
13. RESTful API: https://aws.amazon.com/tw/what-is/restful-api/.
14. X. Zhao and Y.W. Si, “NFTCert: NFT-Based Certificates with Online Payment Gateway,” *2021 IEEE International Conference on Blockchain*, pp. 538-543, 2021.