Regular Paper

Communications of the CCISA
Vol. 31 No. 4 Nov. 2025

# 結合區塊鏈與屬性加密之具緊急存取機制的電子病歷架構

楊欣瑀[1]、王智弘[2*]
[1 2]國立嘉義大學
[1] ava217899@gmail.com、[2] wangch@mail.ncyu.edu.tw

## 摘要

隨著醫療資訊化浪潮，電子病歷 (EHR) 已成為取代傳統手寫病歷的趨勢，它賦予了醫生便捷地存取既往病歷的能力，極大地提高了診斷效率。然而，病歷中包含的個人資料與病史屬於高度敏感的隱私資訊，而當前的 EHR 系統在追求效率的同時，往往犧牲了資訊安全。儘管已有眾多研究提出更安全的存取控制系統，但這些方案卻經常忽略了臨床醫療環境中對於彈性與即時存取的關鍵需求。

為此，本研究提出一套整合了區塊鏈 (Blockchain)、階層式屬性加密 (FH-CPABE)、可信執行環境 (TEE) 以及 星際檔案系統 (IPFS) 的新型電子病歷存取控制系統。我們設計了普通與緊急雙模式遮罩授權機制，旨在確保資料安全的同時，特別兼顧臨床救治過程中的即時存取需求與系統彈性。此外，本系統透過採用代理解密技術來分擔解密運算，從而顯著減輕使用者端設備的負擔，提升運作效率。所有授權決策與操作歷程皆記錄於區塊鏈中，以達成資料保護、操作稽核及運作效率三者間的關鍵平衡。

**關鍵詞：區塊鏈、階層式屬性加密、可信執行環境、電子病歷、存取控制、星際檔案系統**

* 通訊作者 (Corresponding author.)
該論文於第三十五屆全國資訊安全會議 (CISC 2025) 上進行口頭發表。

Regular Paper

Communications of the CCISA
Vol. 31 No. 4 Nov. 2025

# An Electronic Medical Record Architecture Integrating Blockchain and Attribute-Based Encryption with Emergency Access Mechanism

Xin-Yu Yang [1], Chih-Hung Wang [2*]
[1 2] National Chiayi University
[1] ava217899@gmail.com 、[2] wangch@mail.ncyu.edu.tw

## Abstract

The digitization trend in healthcare has led to Electronic Health Records (EHRs) largely replacing traditional handwritten medical charts, granting physicians easy access to patients' past medical histories to aid diagnosis and vastly improving efficiency. However, medical records contain highly sensitive private information, and current EHR systems often compromise information security in their pursuit of efficiency. Although numerous proposals for secure EHR access control systems exist, many overlook the critical need for flexibility and real-time access inherent in the clinical healthcare environment.

To address this challenge, this study proposes a novel EHR access control system that integrates Blockchain, Hierarchical Attribute-Based Encryption (FH-CPABE), Trusted Execution Environment (TEE), and the InterPlanetary File System (IPFS). We introduce a Dual-Mode Masking Authorization Mechanism (Normal and Emergency) designed to ensure data security while specifically accommodating the demand for immediate access and system flexibility necessary during critical clinical rescue processes. Furthermore, the system utilizes Proxy Re-encryption technology to offload complex decryption computations, significantly reducing the burden on user devices and improving operational efficiency. All authorization decisions and operational histories are securely recorded on the Blockchain, thus achieving a vital balance among data protection, operational auditability and efficiency.

**Keywords: Blockchain, Hierarchical Attribute-Based Encryption (FH-CPABE) , Trusted Execution Environment, Electronic Medical Record, Access Control, InterPlanetary File System**

## 壹、前言

資訊化浪潮正快速推動全球醫療邁向「無紙化」。世界衛生組織 (WHO) 在 2025 年世界衛生大會再次延長《全球數位健康策略》，並指出已有 129 個國家制定國家級數位健康藍圖，顯示電子病歷 (Electronic Medical Record, EMR) 已被視為韌性醫療體系的核心基礎設施 [1]。與紙本病歷相比，EMR 能長期、結構化地保存臨床資料，支援跨機構調閱與決策支援，已被 WHO 列為強化初級照護與實現全民健康覆蓋的優先項目。在臺灣，政府自 2009 年啟動「加速醫院實施電子病歷計畫」，迄今已完成雲端交換平台 (EEC) 與健康存摺等基礎建設。衛福部資料顯示，截至 2024 年 7 月，全國共有 356 家醫院完成與電子病歷交換中心 (EEC) 介接 [2]；另有業界調查指出，加入電子病歷交換中心的醫院及診所比例已突破 90%，形成高密度的互通網路 [3]。同時，衛福部計畫在兩年內以 FHIR 標準整合 23 家醫學中心資料，將透過「資料統一」、「規則統一」、「應用程式統一」三大核心策略，打造完善的醫療數據生態系統，確保數據順暢交換，提升醫療決策的準確性與行政效率 [4]。這些數據顯示台灣 EMR 普及度已達國際領先水準，但在標準化與資訊安全上仍面臨挑戰。文獻亦驗證 EMR 對醫療品質的正面效益：2024 年一項針對 591 名護理人員的跨國調查顯示，導入 EMR 後藥物給藥錯誤平均下降約 30%，同時減輕一線人員工作負荷 [5]；系統性回顧則指出，門診單位導入 EMR 能顯著減少處方劑量錯誤及文件遺漏，並在多數場域縮短病人等待時間 [6]。綜上所述，台灣 EMR 已具高覆蓋率與交換基礎，但仍需要在跨院即時存取、安全稽核與彈性授權間取得更佳平衡。

然而，隨著醫療資料數位化的加速，EMR 系統在保障敏感資訊安全的同時，也面臨臨床急救時即時存取的挑戰。目前多數醫院為了病患隱私，普遍採用嚴格的存取控制與授權流程；雖降低了外洩風險，卻可能導致急診醫護無法及時取得完整病歷，影響臨床決策與治療效率。現行細粒度加密方案如屬性加密 (Attribute-Based Encryption, ABE)，特別是密文策略屬性加密 (CP-ABE)，雖能嵌入存取政策，但難以直接應對醫院多層級權限管理需求。雖然階層式屬性加密 (File Hierarchy CP-ABE, FH-CPABE) 改善了多層次資料共享效率，但緊急狀況下往往需透過預設的「急診金鑰」繞過原有政策，此類方案缺乏嚴格條件控管與完整稽核，存在濫用風險。整體而言，現行 EMR 體系亟需一套兼顧資料保護強度、臨床即時可用性與系統效率的整合式解決方案。

基於此，本研究提出並實作一個以 FH-CPABE 為核心的雙模式(普通/緊急)授權架構，並引入「遮罩解密」控制機制，以同時滿足日常與急診需求。具體貢獻包括：(1) 雙模式 FH-CPABE 授權架構：整合普通與緊急模式，支援部門與職級的精細權限管理，並透過可信執行環境 (TEE) 及區塊鏈技術，確保解密僅在合法條件下進行，防範未經授權的越權存取；(2) 普通與緊急雙模式遮罩機制：在普通模式下依嚴格屬性政策控管；緊急模式則透過附加的「急診」屬性與遮罩密鑰控制，使急診醫師僅在符合條件並經

TEE 釋出密鑰時才能解密，兼顧「Break-Glass」即時性與防濫用；(3) 遮罩機制效能評估：實驗證明遮罩解密在即時性與安全性間取得平衡，授權時間顯著縮短，且仍維持高度安全性；(4) 系統擴充與整合構想：結合 TEE 作為硬體信任根，區塊鏈提供不可竄改的稽核日誌，並透過星際檔案系統 (IPFS) 強化加密病歷的分散式儲存。雖然部分模組尚屬設計階段，但為未來建構完整 EMR 安全存取生態奠定基礎。

## 貳、文獻探討

屬性加密 (Attribute-Based Encryption, ABE) 的研究起源於 2002 年。Gentry 與 Silverberg 在 ASIACRYPT 2002 提出了階層式身分加密 (HIBE)，實現多層級私鑰下放並可抵抗合謀攻擊 [7]；Horwitz 與 Lynn 同年進一步形式化其安全定義 [8]。2005 年，Sahai 與 Waters 引入模糊身分加密 (Fuzzy IBE)，允許使用者屬性集合與密文屬性部分重合即可解密，拓展至生物特徵等應用 [9]。隨後，Goyal 等人 (2006) 提出金鑰政策屬性加密 (KP-ABE)，由使用者私鑰決定存取政策 [10]；而 Bethencourt 等人 (2007) 則提出密文政策屬性加密 (CP-ABE)，將政策置於密文中，使加密者可直接決定存取規則，實現細粒度控制並推動實際應用 [11]。然而，隨著雲端與企業級系統需求增加，傳統 CP-ABE 在多層次文件管理上顯得不足。Wang 等人於 2016 年提出文件層級 CP-ABE (FH-CP-ABE)，利用層次模型與傳輸節點機制整合多層次策略，使得一次運算即可解密同一授權範圍內的多個檔案，大幅降低計算與存儲開銷 [12]。此後，研究者持續改進 FH-CP-ABE，例如 Zhang 與 Zhang (2021) 引入動態特權管理與雲端委託解密，提升靈活性與效率 [13]；劉帥南等人 (2023) 則設計分級訪問結構，確保不同安全層級用戶僅能存取相應資料，消除越權風險並降低計算與存儲成本 [14]。整體而言，屬性加密自 HIBE、Fuzzy IBE、KP-ABE、CP-ABE 逐步演進至 FH-CP-ABE，技術已朝向更大規模、更細緻化的應用發展。

在電子病歷 (EMR) 存取控制領域，傳統上廣泛應用角色基存取控制 (RBAC)，透過角色簡化授權管理 [15]，但在臨床情境中難以處理時空條件、權限委派及跨組織協作 [16]。因此，研究逐漸轉向屬性基存取控制 (ABAC)，以使用者屬性、資源屬性與環境上下文來細化政策，例如 Oliveira 等人提出的 AC-ABAC 模型，允許在急診情境中動態調整條件以支持即時存取 [17]。近十年來，ABE 更被廣泛引入 EMR 與個人健康紀錄 (PHR) 雲端存取控制架構：2016 年的研究展示了 CP-ABE 行動 PHR 原型，患者可自訂存取策略，醫護人員僅能在符合條件時解密 [18]；2020 年，Lee 等人提出支援金鑰濫用防護與可驗證外包解密的醫療資料分享系統，以降低雲端代解密的風險與負擔 [19]；2023 年，Gupta 等人提出 SP-MAACS，引入多授權中心 (MA-ABE)，解決集中式架構的單點失效與隱私問題，展現更佳延展性 [20]。

針對急診等「Break-Glass」需求，學界也提出多種方案。Oliveira 等人設計基於 CP-ABE 的 Break-Glass 協議，允許急診團隊臨時解密資料，並在緊急事件結束後撤銷權限 [21]；Saberi 等人結合區塊鏈與 ABAC，提出區塊鏈式 Break-Glass 概念模型，提升透明度與安全性 [22]；Song 等人則將區塊鏈與 Intel SGX 可信執行環境 (TEE) 結合，提出 BTSES 框架，確保 EMR 資料來源的真實性與隱私完整性 [23]。這些研究多以 CP-ABE 為核心，並透過區塊鏈、TEE 與多授權中心等技術增強，重點放在如何兼顧緊急存取的即時性與後續可稽核性。

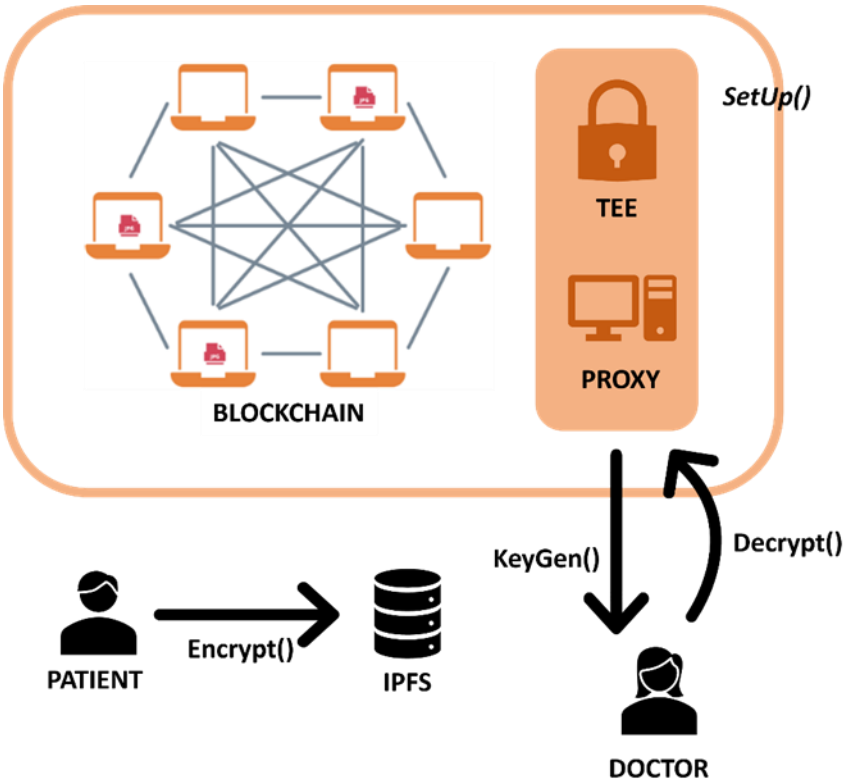
屬性加密技術從基礎理論到多層次 FH-CP-ABE 的發展，已成為 EMR 存取控制的關鍵密碼學工具；同時，透過 ABAC 框架與 Break-Glass 機制的結合，醫療資訊系統正逐步實現「既能保障資料安全，又能滿足臨床即時需求」的雙重目標。

## 參、方法

我們提出了一種階層式存取控制與緊急解密越權能力 FH-CPABE 方案，並以 TEE (Trusted Execution Environment) 搭配 Blockchain 技術構成可信解密授權環境，確保私密資料在必要時能有條件地被安全讀取，同時防止任意越權或重複使用金鑰的風險。整體設計兼顧存取彈性與安全性，適用於需精細化授權管理的場域。

### 3.1 架構

在本系統中，我們設$e: G_0 \times G_0 \rightarrow G_T$為一個雙線性映射，其中$G_0$為質數階$p$之雙線性群，生成元為$g$。任一屬性集$S \subseteq \tilde{A}$ (屬性總集)，使用的兩個雜湊函數分別為：$H_1: \{0,1\}^* \rightarrow G_0$ 及$H_2: \{0,1\}^* \rightarrow G_T$。




圖一：可緊急授權之電子病歷安全存取系統架構圖

對參與角色及負責部份可以參考圖一以及下列補充： 使用者 (User)，在我們假設的環境下通常為醫護人員，持有屬性及金鑰 sk，在滿足策略 (Policy) 的前提下，可以解開密文 CT。資料擁有者 (Data Owner，DO) 一般是病患，他們是病歷的主人，由他們來生成對稱式密鑰$Ksym$來加密病歷，並上傳到到 IPFS 等待下載。代理 (PROXY) 是半信任的機構，主要負責計算加解密部份。TEE 在本文代表了一種可信任的執行環境，他負責為祕密提供機密性跟完整性，我們使用他保管主秘鑰 MK，以其一些其他的機密。區塊鏈在此處負責控管急診解密的合規性以及對所有授權紀錄留痕，方便審計。儲存系統我們採用分散式檔案系統 (IPFS)，他負責保存數量龐大的加密病歷並回傳 CID 來提供檢索，相較於傳統存儲案他還有高速的下載速度跟避免單點故障的能力。

### 3.2 初始化

在系統啟動階段，我們輸入一個安全參數 κ，並由 TEE 隨機選擇 α,β∈Z_p，執行 Setup 程式，生成公鑰 (PK) 與主密鑰 (MSK)：

$$PK = \{\mathbb{G}_0, g, h = g^{\beta}, e(g,g)^{\alpha}\} \quad (1)$$

$$MSK = \{g^{\alpha}, \beta\} \quad (2)$$

### 3.3 金鑰生成

使用者向 TEE 提交自己的屬性組 S 後，TEE 首先為使用者生成$sk \in \mathbb{Z}_p$，並選擇隨機數$r', r_j'$，做$r = \frac{r'}{sk}$跟$r_j = \frac{r_j'}{sk}$，此處參考 [13] 設計。完成後，TEE 開始生成金鑰$D, D_j, D_j'$，具體公式如下所示：

- 金鑰主體：

$$D = g^{\frac{\alpha}{sk}} \cdot h^{r} \quad (3)$$

- 屬性金鑰(對每個屬性 $j \in S$)：

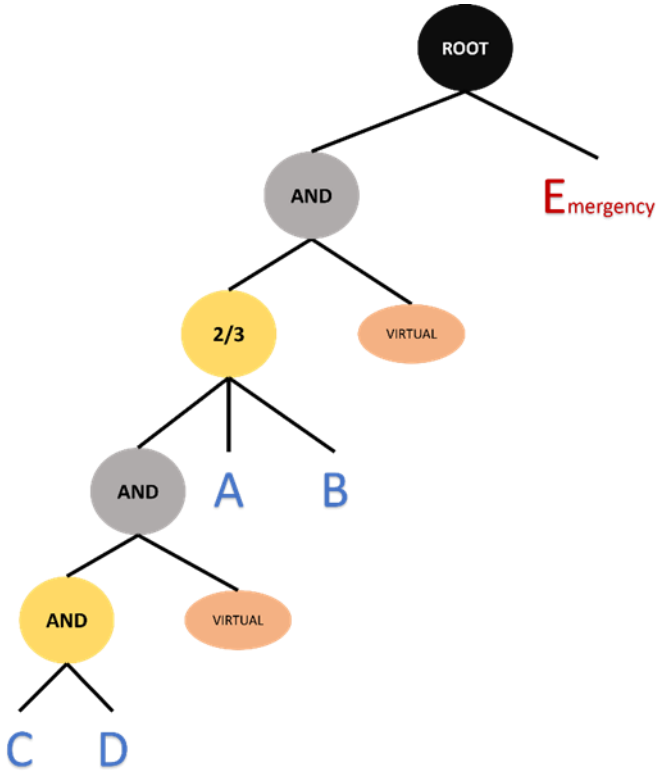
$$D_j = g^{r} H_1(j)^{r_j} \quad (4)$$

$$D_j' = h^{r_j} \quad (5)$$

生成完畢後，TEE 將 sk 分發給使用者保管，將$D, D_j, D_j'$傳送給 PROXY 保管，並將屬性 j=急診時的$D_j, r_j$記錄下來，留待後用。

### 3.4 加密

加密階段，資料持有者 (DO) 將之前加密病歷的對稱式密鑰$K_{sym}$們作為$ck_{i(i=1\sim n)}$傳送給 TEE，TEE 按照不同之$K_{sym}$加密的病歷的敏感程度，依據預先定義的存取控制樹 (Access Tree) 結構，在構建存取控制樹的部分，我們引入了 [14] 的控制節點(灰色 And)跟屬性集不包含的虛擬屬性(橘色葉節點)來防止可能的越權訪問，如圖二，來進行階層式加密。




圖二：存取控制樹

為了生成主要密文，TEE 對 i=1~n 的$ck_i$生成了 n 個$s_i \in \mathbb{Z}_p$來進行加密，加密出 n 份的$\tilde{C}_i, C'_i$密文組，公式如下:

$$\tilde{C}_i = ck_i \cdot e(g,g)^{\alpha \cdot s_i} \quad (6)$$

$$C'_i = g^{s_i} \quad (7)$$

接下來要計算 Access Tree 裡面葉節點的密文組$C_{(x,y)}$, $C'_{(x,y)}$，與經典的 FH-CPABE 不同的是，我們在這裡需要對葉節點屬性為急診的密文組進行遮罩處理，如下列公式:

- 普通屬性

$$C_{(x,y)} = h^{q_{x(0)}} \quad (8)$$

$$C'_{(x,y)} = H_1\big(attr(x,y)\big)^{q_{x(0)}} \quad (9)$$

- 急診屬性

$$C_{(x,y)} = h^{q_{x(0)}} \tag{10}$$

$$C'_{(x,y)} = H_1\big(attr(x,y)\big)^{q_{x(0)}} . g^{tq_x(0)} \tag{11}$$

其中，$g^{t.r_j}$是急診$C'_{(x,y)}$的遮罩值，$t \in \mathbb{Z}_p$是由 TEE 隨機生成的，他會對急診屬性的密文$C'_{(x,y)}$進行遮罩後，將含有遮罩後急診屬性密文$C'_{(x,y)}$的 CT 送上去區塊鏈，供 USER 取用。

最後一組密文是層級節點密文，他們是用來解密較低層的祕密的密文，我們令傳輸節點 x 的子門限集為 TN-CT(x)=$\{ch_1, ch_2, \dots, ch_n\}$，對每個$ch_j$選擇隨機值$\varphi_j$並計算，此處參考 [14] 的設計:

$$\hat{C}_{(x,y),j} = e(g,g)^{\alpha\left(q_{ch_j}(0)+H2\left(e(g,g)^{\alpha q_x(0)}\right)\right)} \cdot e(g,g)^{\varphi_j \cdot H^2\left(e(g,g)^{\alpha q_x(0)}\right)}) \tag{12}$$

$$\check{C}_{(x,y),j} = g^{\alpha+\varphi_j} \tag{13}$$

最後 TEE 將所有密文組件整合輸出成$CT = \{\tau, \tilde{C}_i, C'_i, C_{(x,y)}, C'_{(x,y)}, \hat{C}_{(x,y),j}, \check{C}_{(x,y),j}\}$，完成密文 CT 生成後，TEE 將 CT 結合前面上傳加密病歷獲得的內容識別碼 CID，傳到鏈上記錄，提供使用者下載。

### 3.5 解密

本方案將解密程序劃分為兩個階段，分別為 Proxy 代理解密跟 User 金鑰還原兩部分來進行最終解密，具體流程如下所述:

- Proxy 代理解密：

在此階段，Proxy 負責根據密文 CT 以及授權金鑰$D, D_j, D'_j$來進行階層式解密，以下是具體流程:

對節點 (x,y)，如果他是葉節點，我們需要先跟區塊鏈的通知來判斷使用者需要進行的是普通解密還是急診解密，如果是普通解密的話公式如下:

$$DecryptNode\big(CT, Keys, (x,y)\big) = \frac{e\big(D_j, C_{(x,y)}\big)}{e\big(D'_j, C'_{(x,y)}\big)} = e(g,g)^{r\beta q_x(0)} \tag{14}$$

但是如果在急診解密流程，因為我們之前曾經對急診的$C'_{(x,y)}$乘上遮罩值$g^{tq_x(0)}$，所

以為了解除遮罩，我們必須向 TEE 請求解遮罩密鑰$D_e$，TEE 會計算$D_e = D_j \times g^{tr_j}$後將他傳給 PROXY，此時，PORXY 要用新的$D_e$來取代$D_j$來作運算，才能解開祕密，公式如下:

$$DecryptNode\big(CT, Keys, (x,y)\big) = \frac{e\big(D_e, C_{(x,y)}\big)}{e\big(D'_j, C'_{(x,y)}\big)} = e(g,g)^{r\beta q_x(0)} \tag{15}$$

如果節點 (x,y) 不是葉節點的情況下，我們會使用拉格朗日插值法不斷遞歸計算，直到算出節點 (x,y) 所在的子樹的根節點，也就是第 i 層祕密的節點，並算出$A_i$。

$$\begin{aligned} A_i = DecryptNode\big(CT, Keys, (x_i, y_i)\big) &= \frac{e\big(D_j, C_{(x,y)}\big)}{e\big(D'_j, C'_{(x,y)}\big)} = e(g,g)^{r\beta q_x(0)} \\ &= e(g,g)^{r\beta s_i} \end{aligned} \tag{16}$$

然後我們可以計算出$e(g,g)^{\alpha s_i}$，但因為我們在前面有對參數進行除以 sk 的處理，所以此刻我們真正能計算出來的是:

$$F'_i = \frac{e(C'_i, D)}{A_i} = e(g,g)^{\frac{\alpha}{sk} \cdot s_i} \tag{17}$$

PROXY 會將$F'_i$傳遞給使用者來進行最後的解密。

- User 金鑰還原

進入在第二階段，使用者從 Proxy 獲得$F'_i$並解出$F_i = (F'_i)^{sk} = e(g,g)^{\alpha \cdot s_i}$，如此我們可以進行下一步運算來解出$ck_i$：

$$\frac{\tilde{C}_i}{F_i} = \frac{(ck_i \cdot e(g,g)^{\alpha \cdot s_i})}{e(g,g)^{\alpha \cdot s_i}} = ck_i \tag{18}$$

使用者成功復原對應之$ck_i$，完成加密資料的解密程序。

最後，階層式 CPABE 的特色即是，高層的解密者，可以推出低層的祕密，反之不然，因此我們參考 [14] 的公式來對低層的祕密進行推算:

$$F_{i+1,j} = \frac{\hat{C}_{(x,y),j}}{e\left(\check{C}_{(x,y),j}, g\right)^{H_2(F_i)}} = e(g,g)^{\alpha q_{chj(0)}} \tag{19}$$

## 肆、結論

本研究提出之基於區塊鏈與可信執行環境輔助的層級式屬性加密電子病歷存取架構，有效兼顧了資料安全、存取效率及緊急應變能力。未來可進一步整合跨鏈授權管理與行為風險偵測，強化系統彈性及防護層級，以應對更為複雜多變的醫療資訊應用場景。

## 參考文獻

[1] World Heaalth Organization, https://www.who.int/news/item/23-05-2025-seventy-eighth-world-health-assembly---daily-update--23-may-2025

[2] Ministry of Health and Welfare, https://emr.mohw.gov.tw/myemr/Html/Introduction

[3] CIO Taiwan, https://www.cio.com.tw/interview-pang-yiming-director-of-information-services-at-the-department-of-health/

[4] United Daily News , https://udn.com/news/story/7266/8602521

[5] R. Naamneh and M. Bodas, “The effect of electronic medical records on medication errors, workload, and medical information availability among qualified nurses in Israel: a cross-sectional study,” *BMC Nursing*, vol. 23, no. 1, Art. no. 270, 2024, doi: 10.1186/s12912-024-01936-7.

[6] S. Albagmi, “The effectiveness of EMR implementation regarding reducing documentation errors and waiting time for patients in outpatient clinics: A systematic review,” *F1000Research*, vol. 10, Art. no. 514, 2021.

[7] C. Gentry and A. Silverberg, “Hierarchical ID-based cryptography,” *in Advances in Cryptology—ASIACRYPT 2002*, Lecture Notes in Computer Science, vol. 2501. Berlin, Germany: Springer, 2002, pp. 548–566.

[8] J. Horwitz and B. Lynn, “Toward hierarchical identity-based encryption,” *in Advances in Cryptology – EUROCRYPT 2002*, *ser. Lecture Notes in Computer Science*, vol. 2332. *Berlin, Germany: Springer*, 2002, pp. 466–481.

[9] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” i*n Advances in Cryptology – EUROCRYPT 2005, vol. 3494, Lecture Notes in Computer Science. Berlin, Germany: Springer*, 2005, pp. 457–473.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. *Computer and Communications Security (CCS), Alexandria*, VA, USA, 2006, pp. 89–98.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *in Proc. IEEE Symp. Security and Privacy*, Oakland, CA, USA, May 2007, pp. 321–334.

[12] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1265–1277, Jun. 2016.

[13] J. Zhang and W. Zhang, "An improved FH-CP-ABE scheme with flexible attribute management and efficient user decryption," *Int. J. Netw. Security*, vol. 23, no. 5, pp. 856–866, Sept. 2021.

[14] S.-N. Liu, B. Liu, Z. Guo, C. Feng, Z. Qin, and Y. Qing, "File Hierarchy CP-ABE Scheme Supporting Graded User Access," *Journal of Software*, vol. 34, no. 7, pp. 3329–3342, Jul. 2023.

[15] M. A. de Carvalho Junior and P. Bandiera-Paiva, "Health Information System Role-Based Access Control: Current Security Trends and Challenges," *Journal of Healthcare Engineering*, vol. 2018, Article ID 6510249, 2018.

[16] M. Jayabalan and T. O'Daniel, "Access control and privilege management in electronic health record: A systematic literature review," *J. Med. Syst.*, vol. 40, no. 12, Art. no. 261, Dec. 2016.

[17] M. T. D. Oliveira, Y. Verginadis, L. H. A. Reis, E. Psarra, I. Patiniotakis, and S. D. Olabarriaga, "AC-ABAC: Attribute-based access control for electronic medical records during acute care," *Expert Systems with Applications*, vol. 213, Art. no. 119271, 2023.

[18] H. Hong, D. Chen, and Z. Sun, "A practical application of CP-ABE for mobile PHR system: A study on the user accountability," *SpringerPlus*, vol. 5, no. 1, Art. no. 1320, 2016.

[19] Y. W. Hwang and I. Y. Lee, "A study on CP-ABE-based medical data sharing system with key abuse prevention and verifiable outsourcing in the IoMT environment," *Sensors*, vol. 20, no. 17, Art. no. 4934, 2020.

[20] R. Gupta, P. Kanungo, N. Dagdee, G. Madhu, K. S. Sahoo, N. Z. Jhanjhi, M. Masud, N. S. Almalki, and M. A. AlZain, "Secured and privacy-preserving multi-authority access control system for cloud-based healthcare data sharing," *Sensors*, vol. 23, no. 5, Art. no. 2617, 2023.

[21] M. T. de Oliveira, A. Bakas, E. Frimpong *et al.*, "A break-glass protocol based on ciphertext-policy attribute-based encryption to access medical records in the cloud," *Ann. Telecommun.*, vol. 75, no. 2, pp. 103–119, Apr. 2020.

[22] M. A. Saberi, M. Adda and H. Mcheick, "Towards an ABAC Break-Glass to access EMRs in case of emergency based on Blockchain," 2021 *IEEE International Conference on Digital Health (ICDH)*, Chicago, IL, USA, 2021, pp. 220-222.

[23] Z. Song, H. Gao, Z. Liu, H. Lei, and Y. Zhou, “BTSES: A Blockchain and TEE Enabled Secure EMR Sharing Solution,” in *Proc. 14th Int. Conf. Computer Engineering and Networks (CENet)*, Singapore, 2024, Lecture Notes in Electrical Engineering, vol. 1387, Springer, 2025.