BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

原始研究

使用區塊鏈與功能偏置橢圓曲線的安全可靠霧化架構加密演算法的安全可靠霧聯網架構

Charu Awasthi, PhD Student[1]; Satya Prakash Awasthi, PhD[2]; and Prashant Kumar Mishra, PhD[3]

[1]印度齋浦爾 Poornima 大學電腦工程系研究學者；[2]印度齋浦爾 Poornima 大學電腦工程系副教授；[3]印度坎普尔 Pranveer Singh 技術學院電腦科學與工程系副教授

通訊作者：Charu Awasthi，電子郵件： charuawasthi@gmail.com DOI:

https://doi.org/10.30953/bhty.v7.347

Keywords: blockchain, FB-ECC, fog computing, functional biased elliptic curve cryptography algorithm, galactic bee colony optimization algorithm, GBCOA, healthcare services

摘要

霧狀運算 (FC) 是一種新興技術，可作為雲端與裝置之間的橋梁，擴展雲端運算網路的能力與效率。Fog 裝置可在本機處理大量資訊，可攜式運輸，並可部署在各種系統上。由於其即時處理與事件反應的特性，非常適合醫療照護。由於具有如此廣泛的特性，新的安全性與隱私權問題也隨之而來。由於安全傳輸、抵達和存取，以及醫療裝置的可用性，安全性在醫療照護領域產生了新的問題。因此，相較於標準的雲端運算方法，FC 需要獨特的安全與隱私指標方法。因此，本文提出一種有效的區塊鏈，取決於 FC 中的安全醫療服務。在此，霧節點收集來自醫療感應裝置的資訊，並使用區塊鏈網路中的智慧契約來驗證這些資料。我們提出一種功能偏向的橢圓曲線加密演算法來加密資料。使用銀河蜜蜂群落最佳化演算法進行最佳化，以強化加密的程序。建議方法的效能經過評估，並與傳統技術進行對比。結果證明，FC 與區塊鏈的結合提高了醫療服務中資料傳輸的安全性。

提交：2024 年 8 月 7 日；接受：2024 年 10 月 4 日；發表：2024 年 12 月 31 日

近年來，電子通訊的突破性發展改變了物聯網 (IoT)，創造出可利用並連結物聯網的小家電。控制資訊的收集與分享。這些技術創造出微小、具成本效益且功能較弱的多功能感測系統，能夠觀察和傳送運輸、醫療照護和工業等多個領域的不同資料(1)。

醫療照護物聯網提供多項優勢，包括即時模式的資料傳輸，以及控制病患不同時間生理狀況的能力。設備，包括葡萄糖計、物聯網可讓醫療服務提供者在本地收集病患的健康資料，並根據病患的健康資訊做出決策。

診所實施物聯網已有數年時間，現在他們已在病患照護室及其系統中安裝醫療照護物聯網裝置。然而，臨床機構、診所和企業並未正視連結至區域網路或廣域網路的醫療照護物聯網的親防威脅。由於驗證與編碼技術薄弱，IoT 裝置很容易被挾持，導致各種疑慮。

因此，在醫療照護物聯網中，區塊鏈是為了安全與可信賴的傳輸而推出。圖 1 展示霧狀運算 (FC) 的架構。

物聯網系統的發展，尤其是在醫療保健產業，產生了大量的資訊，這些資訊會被傳輸到雲端並儲存起來。由於需要即時處理和儲存資訊，處理如此大量的雲端資訊造成了瓶頸。

雲端資訊的保護也是一個重要的問題。[2]FC 的構想就是為了解決這個問題所做的嘗試。霧運算是雲端運算系統的延伸。陪伴雲端運作是 Fog 的主要角色。例如，Fog 將計算資源傳送至較接近網路邊緣的裝置。典型的 IoT 雲端架構在擴充性和可靠性方面有問題，但 FC 可以解決這樣的問題。

如圖 1 所示，由於霧節點在網路邊緣運作，且地理位置較為分散，因此可改善資訊保護與預防，並將延遲減至最低，這對於醫療資訊等應用而言至關重要。雲端總頻寬也可降至最低，進而改善服務品質。[3]為了解決這個問題，我們提出了一個使用區塊鏈與 FC、功能性偏置橢圓曲線加密演算法 (FB-ECC) 的霧化架構，用於醫療照護服務。

相關工作

本文針對資料加密提出 FB-ECC 演算法，並使用 galac-tic bee colony optimization algorithm (GBCOA) 進行最佳化。此演算法

演算法與不同文章中提出的各種演算法進行比較，以分析其效能。

表 1 列出研究人員對於霧化架構相關觀察的頂線觀察結果。相關文獻總結顯示，如果我們能夠結合適當的演算法，利用 IoT 裝置的區塊鏈功能來整合霧系統架構，將是一個有趣的領域。

Ngabo等人[4]指出，他們工作的主要目標是發展防護機制，以對抗由物聯網感測層與雲端資料庫資訊儲存所產生的醫療資料挖掘攻擊。使用 ECC 數位簽章來協助分散式帳本資料庫（伺服器）的公開授權區塊鏈保護程序，以提供不可變更的保護與傳輸清晰度，並在物聯網的霧層保護病患資訊遭篡改。

Baniata 和 Kertesz[5]對 FC-block chain（FC-BC）組合--FC- BC 組合的技術現況--進行了徹底的文獻分析和分類。作者根據出版年份和領域，以及所採用的演算法、BC 功能和 BC 在 FC 架構設計中的位置，來討論和組織相關工作。作者詳細介紹了 BC-FC 組合的研究、評估和未來的困難。

Tariq 等人[6]嘗試在未來數位基礎設施保護仍處於開發階段時解決問題。隨著產生大量資訊的 architec-ture 的到來，建立了依功能而定的霧架構。

此外，還討論了霧化 IoT 裝置的額外保護需求，以及與霧化 IoT 相關的 FC 保護挑戰和大量資訊機密性。接著，考慮互補性的

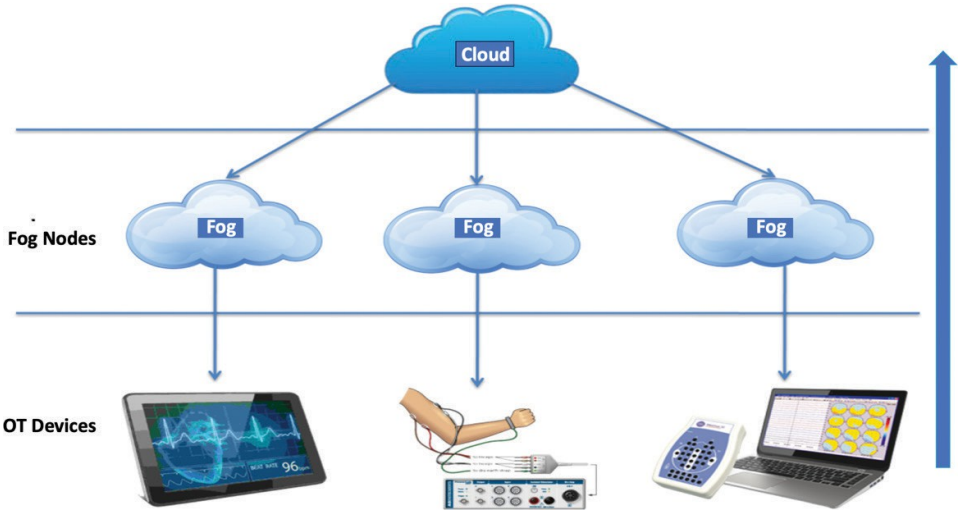

圖 1. 霧運算架構。

引用：Blockchain in Healthcare Today 2024, 7: 347 - https://doi.org/10.30953/bhty.v7.347

*表 1.*霧運算架構領域研究人員的觀點

資料來源	頂線觀測
Ngabo 等人[4]	主要目標是針對物聯網感測層與雲端資料庫資訊儲存所產生的醫療資料挖掘攻擊，開發防護機制。
Tariq 及其同事[6]	解決未來數位基礎設施保護的相關問題。
Banerjee 等人[7]	在緊急情況下增強使用者體驗和服務彈性。
Fernández 等人[8]	實施一套系統，將 IoT 功能加入商用 CGM，以實現對病患的遠端監控。
Muthanna 等人[9]	提出一個 SDN 框架，以規範和管理霧節點的邊緣計算層。
Srivastava 等人[10]	討論醫療照護中的 FC、區塊鏈與物聯網
Yánez 等人[11]	提出一種新的情境感知方法，用於物聯網-區塊鏈網路中的鏈上資訊分配。
Kumari 等人[12]	Pareek 等人(13) 檢視了霧與雲端運算以及 IoT 在提供終端使用者持續情境感知服務方面的功能。
Pareek 等人[13]	觀察到物聯網將全球許多小工具連結起來。
Hanumantharaju 等人[14]	指出物聯網可協助病患與醫療照護提供者保持聯繫，並提供社區明確、有價值的照護。
Mayer 等人[15]	提出一種 FC 架構範例，將區塊鏈、霧狀運算與物聯網整合至醫療照護領域。

FC：霧狀運算；CGM：持續葡萄糖監測；IoT：物聯網；SDN：軟體定義網路：物聯網；SDN：軟體定義網路。

本研究將討論區塊鏈與 FC 之間的相互依存關係，以及它們在解決 IoT 中各種防護疑慮方面所扮演的角色。因此，本研究提供了針對霧式深度物聯網系統的攻擊種類分類，比較了該領域在保護服務方面的最新貢獻，並提出了未來研究的建議。

Banerjee 等人[7]增強了使用者體驗與服務在緊急情況下的彈性；FC 技術已被運用於連結物聯網與邊緣網路的即時運算。Fog 邊緣運算的分散設計與接近終端使用者的特性，可為 IoT 使用提供更快速的反應時間與更高品質的服務。FC、物聯網和機器學習包含在研究人員提供的範例的每個部分，以改善醫療照護的品質。區塊鏈技術用於確保架構保護。

Fernández 等人[8]實作了一套系統，將 IoT 功能加入商用連續血糖監測器 (CGM)，以遠端監控病患，並在潛在危險情況下通知病患。為了收集 CGM 的血糖測量數據，使用手機將測量數據傳送至遠方的雲端或霧中的分散節點。此外，還包括一個分散式儲存系統，可收集、處理及儲存所獲得的資訊，以便與醫學科學家、臨床醫師及照護者分享準確、可信及網路安全的資訊。

GlucoCoin 的創建是為了獎勵個人向系統提供新資訊，同時也是一種數位貨幣。此系統使用可執行智慧契約的區塊鏈，可自動購買 CGM 感應器，或補償提供資訊以啟動系統功能的使用者。

C.Awasthi 等人 Muthanna 等人[9]提出一個軟硬體定義網路(SDN)的架構，用以規範與管理霧狀節點的邊緣運算層，並為延遲的物聯網應用提供極佳的可用性與可靠度。在 SDN 網路中使用具有資源限制的 OpenFlow 交換器，該交換器具有分散的控制者。透過使用區塊鏈，可實現可信的去中心化。OpenFlow 交換器將透過資訊卸載技術，依據其目前的工作量來指派計算處理職務。針對整個網路提出了流量模型。該演算法使用模擬和測試平台進行測試。

Srivastava 等人[10]討論了醫療保健中的 FC、區塊鏈和 IoT。與雲端運算（在雲端與稱為物聯網設備的終端使用者裝置之間運作）不同，FC 擴展了雲端運算的能力，以執行跨網際的處理、儲存與互動等功能。它提供了優異的資訊儲存設施，具有即時存取、降低延遲、更高的反應能力、更好的容錯能力，以及受保護的隱蔽環境。在 IoT 系統中，霧層、存取層、資訊互動層、應用層和保護層被分為五個層次。作者強調了區塊鏈技術與共識機制，以改善醫療照護情境中的資訊保護。Yánez 等人[11]提出了一種新的情境感知方法，用於物聯網-區塊鏈網路中的鏈上資訊分配。此外，他們使用模糊邏輯建立了一個資料控制器，可利用幾個情境特徵（例如資訊的 品質與數量，以及其傳送的網路）來估算請求的 RoA 值。此機制的設計與實作也讓兩種熱門的物聯網-區塊鏈技術更臻完美。

引用：Blockchain in Healthcare Today 2024, 7: 347 - https://doi.org/10.30953/bhty.v7.347

架構特色。資料分配方法在依賴區塊鏈的雲端與霧端架構中實體化，並使用霧端匯流排 (Fog Bus) 進行評估，以展示我們方法的功效。他們也使用真實世界的醫療保健用途，將我們的方法與目前的決策流程進行比較。

Kumari 等人[12]研究了霧與雲端運算以及 IoT 在需要時為終端使用者提供連續情境感知服務的功能。針對即時資訊收集、處理與傳輸，他們提出了一個三層的病患驅動醫療照護架構。該架構可為終端使用者提供有關醫療照護 4.0 生態系統中霧設備和閘道在目前和未來用途的使用資訊。

Pareek 等人[13]提到，物聯網將全球許多小工具連結在一起。為了紓緩醫療照護系統的壓力，依賴物聯網的技術可能有助於降低醫療照護的支出，並提升運算與處理速度。在 IoT 中，更多、更複雜的醫療照護資訊集需要使用雲端運算。延遲、頻寬使用、即時存取延遲、安全性與機密性只是將 IoT 與雲端整合時所遇到的幾個問題。談到雲端運算，在評估任何基於 IoT-Fog 的系統模型設計之前，必須先解決許多問題與挑戰。

Hanumantharaju 等人[14]提到，物聯網的角色可能有助於病患與醫療照護提供者保持聯繫，並透過讓雙方更容易保持聯繫，提供社區明確、價值依賴的照護。FC 可作為將 IoT 應用於醫療保健的基礎。專家們討論了醫療保健 4.0。研究人員將從資訊收集與評估、保護與保密，以及電子健康照護服務等方面，探討 FC 分類法如何成為健康照護 4.0 的最佳答案。

Mayer 等人[15]提出了一種 FC 架構範例，將區塊鏈、FC 和物聯網整合在一起，用於醫療保健領域。在大多數情況下，FC 架構及其克服物聯網限制的差異化方法是最重要的貢獻。

相關文獻回顧顯示，若能整合適當的演算法，利用 IoT 裝置的能力來整合霧化架構與區塊鏈，將是一個有趣的領域。

本文提出一種 FB-ECC 資料加密演算法，透過 GBCOA 完成最佳化。本演算法將與不同文章中提出的各種演算法進行比較，以分析其效能。

建議方法

本節將簡單介紹 FC 中一個有效的區塊鏈依賴保護醫療服務

。

霧節點收集來自醫療感應裝置的資訊，並使用區塊鏈網路中的智慧契約來驗證這些資料。為了加密資料，提出了 FB-ECC 演算法。為了優化加密過程，實施了 GBCOA。建議方法的效能經過評估，並與傳統方法進行比較。圖 2 顯示實施技術的流程說明。

在此基礎架構中可偵測到四個層級：物聯網層、區塊鏈霧層、雲層和資料分析層。病人的健康資訊是透過醫療感應裝置取得。透過有線或無線存取媒體 (包括 ZigBee 和 Wi-Fi)，每個 IoT 醫療設備都可以連結到單一 Fog 節點。霧節點實施預設的保護標準，以控制連接的 IoT 裝置和服務，並作為雲端和區塊鏈之間的中介，允許資訊查詢的授權索引。

使用智慧契約進行資料驗證

雖然這個詞之前用於網際網路上陌生人之間的協定，但智慧契約是在 Ethereum 区块鏈上實作的契約範例。智慧型契約有以下規則：

1. 協商協議的條件
2. 自動驗證協議
3. 執行協定的條件

智慧契約由許多功能組成，可從區塊鏈外部或透過其他智慧契約存取。區塊鏈與智慧契約技術的結合使用，使交易各方不再需要依賴集中式系統。由於智慧契約保存在區塊鏈上，因此網路中每個連結的參與者都擁有智慧契約的複製本。當被允許或協定的事件啟動時，智慧契約可執行協定的儲存程序。每個契約轉移以及整個活動的稽核記錄都會依時間順序儲存，以供未來存取。任何一方試圖改變區塊鏈上的合約或交易，都會被所有其他參與者偵測到並阻止。即使其中一方當機，系統仍可繼續運作，不會遺失任何資訊或完整性。因此，一個龐大、安全、合乎邏輯的電腦系統被創造出來，而不會有與集中式範例相關的危險、開支或信任困難。

使用恆星共識協定進行區塊驗證

Stellar 共識協定是一種分散式的共識協定，在此協定中，網路中的節點不需要與其他節點進行協定。

引用：Blockchain in Healthcare Today 2024, 7: 347 - https://doi.org/10.30953/bhty.v7.347

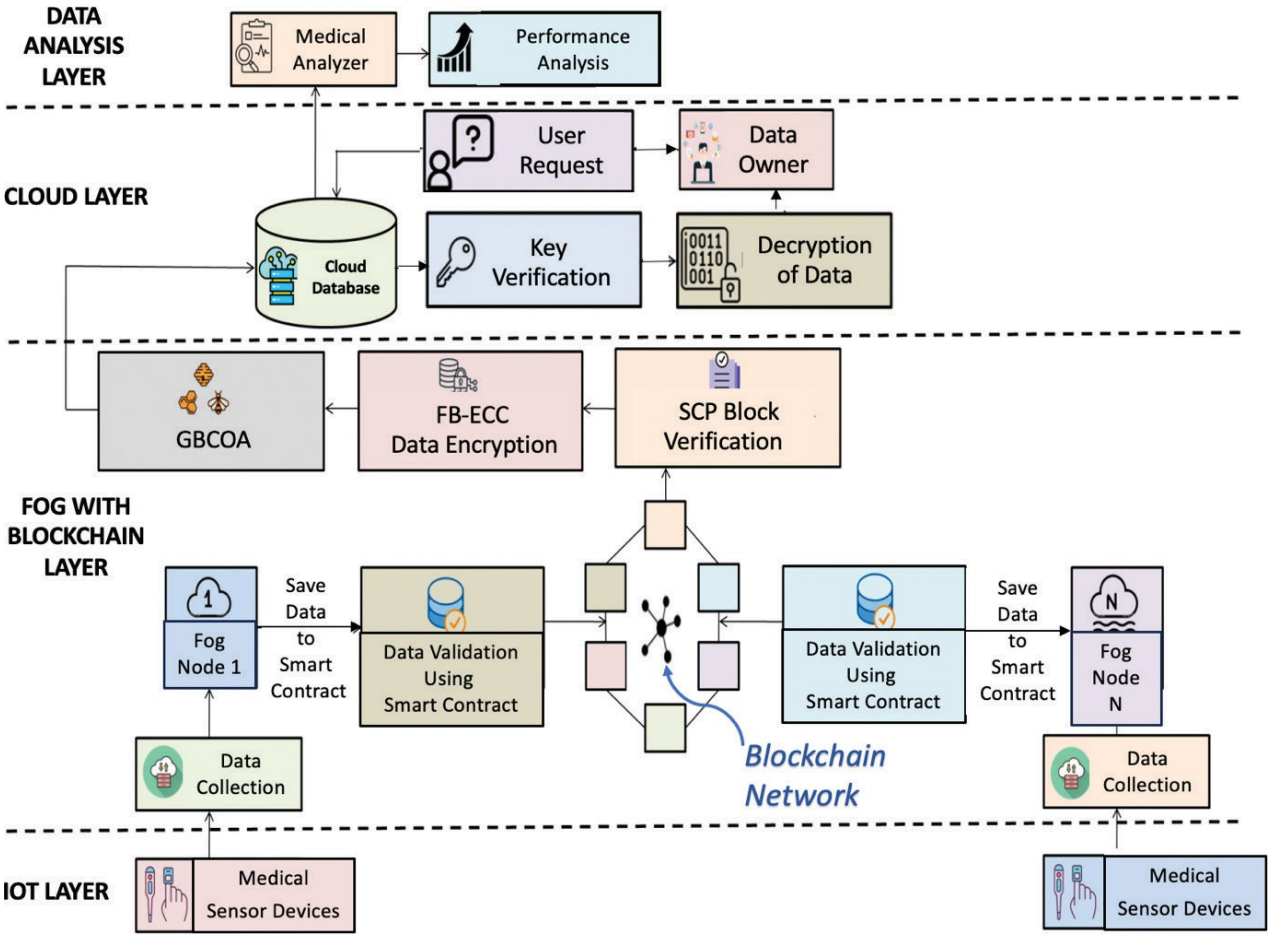

圖 2. 實作技術的 流程圖解。FB-EEC：功能偏置橢圓曲線加密算法；FC-BC：霧狀運算區塊鏈；GBCOA：銀河系蜜蜂群落最佳化演算法，IoT：物聯網。

[16]「quo-rum slice」的概念最初是由此通訊協定所建立，指的是彼此信任的節點集合。法定人數」是一個大到足以建立共識的節點群，而「法定人數分片」則是法定人數的一個子集，說服一個或多個節點同意。

每個取得這些值的節點都會檢查區塊中的單一值，結果單一值就會用來驗證區塊。節點在整個階段中開始檢查區塊是否接受或放棄前一階段選擇的值。如果一組節點無法達成一致，則會將值轉移到更大的區塊進行驗證。

使用功能偏置橢圓曲線加密演算法進行資料加密

FB-ECC 是著名的公開金鑰加密技術，可可靠安全地保護編碼醫療資訊的保密性和機密性。加密和解密使用相同的金鑰 (表 2)。

FB-ECC 是一種常見的公開金鑰加密方法，使用不同的金鑰對進行加密和解密程序，例如隨機建立公開金鑰和私人金鑰。FB-ECC 等公開金鑰加密技術也被整合到這項技術中。新交易的授權和清晰度取決於使用者之間的分散同意（大於 50%），這使得此技術比公鑰密碼技術更具優勢。由於只有 FB-ECC 密鑰才能傳回實際資訊，因此任何未經授權的個人都無法檢索被隱藏的醫療資訊。

在非對稱金鑰密碼術中，FB-ECC 技術在進行公開金鑰密碼術中扮演著重要的角色。此外，利用定義的基 點、曲線和素數函數的最高極限建立一個數字表達式，並利用下列 FB-ECC 方程進行加密：

$$K^2 = L^3 + Bl + C \quad (1)$$

*表 2.*功能偏置橢圓曲線加密演算法

輸入：輸入資料 (dI)、私人密碼匙 (K)。

輸出：加密後的資料 (Ed)。

1: 隨機產生公開金鑰 (Pk)；

2: $P_k = A * G_o$/* 產生 Go 的函數取決於曲線方程式，Go 是從映射函數中抽取出來的。

3: 產生密碼 Cs 為 Cs← RM * Go；

4:加密資料 (E_d) 產生為 $E_d \leftarrow S_M * Pa) + (d_{(P)}, W)$;/* W /* W 表示曲線上的基點。

5:加密後的資料 (E_d) 上傳至公共雲端環境

註： 請參閱正文，以瞭解更詳細的內容。

整數由 b 和 c 表示。然而，加密過程的整體強度取決於每個加密演算法所產生的金鑰。最初的程序是製作用於加密資訊的公開金鑰，通常是從接收者處接收。第二個過程是產生私密金鑰，使接收方能夠解密原始資訊。W 是曲線的起始點，A 是在 1- (m - 1) 的範圍內所選擇的隨機整數：

$$S = A \times W \tag{2}$$

公鑰用 S 表示，私鑰用 A 表示。

加密是一種將實際資訊轉換為密文資訊的方法，它用於

以增加保護。FB-ECC 是雲端安全中最常使用的技術，可提供保護

取決於問題的複雜性。加密程序的強度由金鑰產生的

在此加密過程中，輸入的原始資訊 dI 和私人密碼匙 K 作為輸入，而產生函數 (Go) 則建立公開密碼匙 (Pk)。在此加密過程中，輸入原始資訊 dI 及私人密碼匙 K，並由產生函數 (Go) 產生公開密碼匙 (Pk)。因此，密碼 Cs 是使用 4 位元隨機數 Rm 和 Go 來建立的。輸入資料 dI 接著使用曲線的基點 W 進行編碼，接著產生公開金鑰 Pk 和隨機數 Rm。

Galactic Bee Colony 最佳化演算法

GBCOA 模擬恆星、星系和超星系的運動，在指定的搜尋空間中找出可行的替代方案。就像星系中的恆星一樣，彼此溝通。代理被銀河蜂群分為兩個層次。恆星顯示在第一層，而星系則代表在第二層。除了第二層的起始族群是來自於

在第一層中，每一層都有其搜尋機制。在每個階段，可能會 使用幾種搜尋技術。在所有階段中，研究人員都選擇採用蜂群最佳化方法。因此，在第一層級中，每個子群落都使用 BCO 來尋找最佳答案，然後將其傳送至更高層級以建立超級蜜蜂。在新的 BCO 運行中，超級蜜蜂被用作起始群體，以尋找最佳解決方案。BCOA 多層出擊表示為 (3)：

$$s_q^p \in S : q = 1, 2, ..., M_p$$

$$b_p \in S_{(p)} : b_p = best\left(S_p\right)$$

$$G = \bigcup_{p=1}^{M} b_{(p)} \tag{3}$$

在原始的銀河蜜蜂最佳化技術中，第一個子群 (subpopulation) 的 N 個解隨機產生。S_q^p表示第 i 個子群的第 j 個解。S_p

$b_{(p)}$ (best(S_p)) 表示子群 $S_{(p)}$的最佳解。集合 G 表示由子群最佳解組成的超群。

來自子群的最佳解。

在階段 1 中從每個子群中獲得的較佳解被用作階段 2 的第一個群。第 2 階段執行 L2 次，然後將第 2 階段中識別出的優異結果作為該 epoch 的最終解。整個演算法會運行各次，然後將各次中識別出的優異結果作為演算法的最後一次結果。

雲端資料庫

在此範例下，集中式健康記錄伺服器與醫療記錄儲存庫或資料庫進行通訊。病人擁有資訊，其中包括敏感的個人資訊。患者的醫療記錄通常包含在此類文件中，也可能包括生物特徵資料、生理、心理和精神健康問題、個人病史、過敏症、使用的藥物、病症、先前的醫療治療和疾病等等

引用：Blockchain in Healthcare Today 2024, 7: 347 - https://doi.org/10.30953/bhty.v7.347

。財務資料，包括

使用區塊鏈的虛擬化架

財務資料，包括銀行帳戶、信用卡和借記卡號碼，以及病患的身份，都可能包含在醫療記錄中。

保護電子健康記錄的安全性和機密性被視為健康資訊管理的核心要素。健康資料系統的主要目標是保證資訊在需要時可以存取，並且在儲存或傳送時不會被不當利用、揭露、取得、變更或銷毀。

安全隱私標準共同確保適當的控制和保障措施。在醫療記錄儲存庫或資料庫中，患者 IDen-tification 編號用於識別醫療記錄。根據所述的 ID，患者的醫療保健資訊屬於個人識別資訊。患者資料可能單獨使用，也可能與其他資料一起使用。患者資訊儲存於私有雲端虛擬電腦的資料庫中。

在資訊管理方面，私有雲架構包括運算、儲存和網路服務。將健康資訊傳送至雲端時，會根據私有雲端安全架構進行加密和散列作業。實際的健康記錄資訊保存在一個資料庫中，而加密所需的金鑰則保存在另一個資料庫中。因此，攻擊者存取儲存於雲端電子健康記錄資料庫中重要病患資訊的權限受到限制。因此，建議的架構可透過確保資訊的保密性與完整性來保護病患的敏感資料。因此，醫療照護使用者可隨時隨地解密資料，並存取重要資訊。

效能分析

本文描述了在 FC 架構中使用區塊鏈和功能性偏置 ECC 演算法安全儲存加密醫療資訊的性能評估標準。以金鑰產生時間(KGT)、加密時間(ET)、解密時間(DT)及安全等級來評估此建議演算法系統的受保護儲存部分。此外，等式(4)、(5)及(6)亦提供了估算各種時間的相關公式。

加密時間

加密時間是指加密資訊所需的時間，單位為毫秒。其計算方式如下：

加密時間= 結束時間 - 開始時間

$$KGT = ITT + ET \quad (4)$$

其中 ITT 代表資訊傳輸時間，而 ET 代表加密時間。這裡計算的 ET 是資訊從原始資訊編碼到轉換為加密資訊所花費的時間。其中，ENDT 表示結束時間，STARTT 表示加密程序的開始時間。

$$et = endt - startt \quad (5)$$

圖 3 顯示建議技術利用功能偏置 ECC 方法的加密時間。研究人員發現，加密時間會隨著金鑰位元數變大而增加。另一方面，我們建議的架構所需的加密時間遠少於傳統的方法，如 Advanced Encryption Standard (AES)、Data Encryption Standard (DES) 和 Rivest-Shamir-Adleman (RSA)。

解密時間

解碼加密資訊所需的時間稱為解密時間，其計算方式如下：

解密時間= 結束時間 - 開始時間

在此，DT（解密時間）是以毫秒為單位計算用來解碼加密資訊的資訊所需的時間，並使用公式 (6) 計算。

$$dt = endt - startt \quad (6)$$

圖 4 描述建議架構的解密時間與傳統方式的比較。

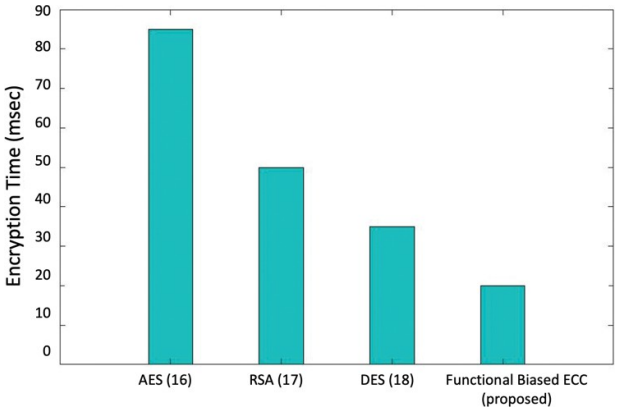

圖 3. 金鑰產生時間分析。AES：進階加密標準 (Advanced Encryp-tion Standard)、DES：資料加密標準 (Data Encryption Standard)、ECC：橢圓曲線加密法 (ellip-tic curve cryptography)、RSA：Rivest-Shamir-Adleman.

引用：Blockchain in Healthcare Today 2024, 7: 347 - https://doi.org/10.30953/bhty.v7.347

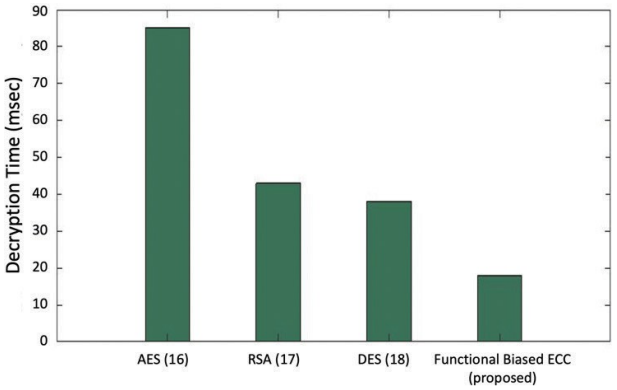

*圖 4.*解密時間分析。AES：進階加密標準 (Advanced Encryption Standard)、DES：資料加密標準 (Data Encryption Standard)、ECC：橢圓曲線加密法 (ellip-tic curve cryptography)、RSA：Rivest-Shamir-Adleman：Rivest-Shamir-Adleman.

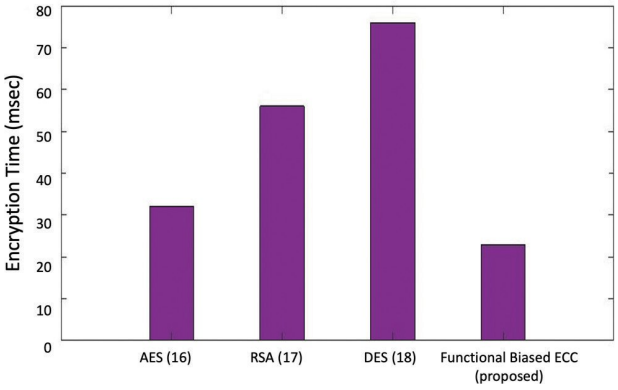

*圖 5.*金鑰產生時間分析。AES：進階加密標準 (Advanced Encryption Standard)、DES：資料加密標準 (Data Encryption Standard)、ECC：橢圓曲線加密法 (elliptic curve cryptography)、RSA：Rivest-Shamir-Adleman：Rivest-Shamir-Adleman.

關鍵字。與 AES、DES 及 RSA 等傳統方法比較，我們建議的方法即使使用較大的金鑰，解碼所需的時間也較短。

金鑰產生時間

從圖 5 可以看出，相較於 AES、DES、RSA 等傳統方法，建議的安全儲存功能偏向橢圓曲線加密演算法所消耗的時間較少。

安全層級

圖 6 將建議的功能偏置 ECC 與傳統安全儲存演算法 (如 DES、RSA 和 AES) 的安全層級進行比較。與傳統方法比較，所提出的替代方案提供更高的安全性。

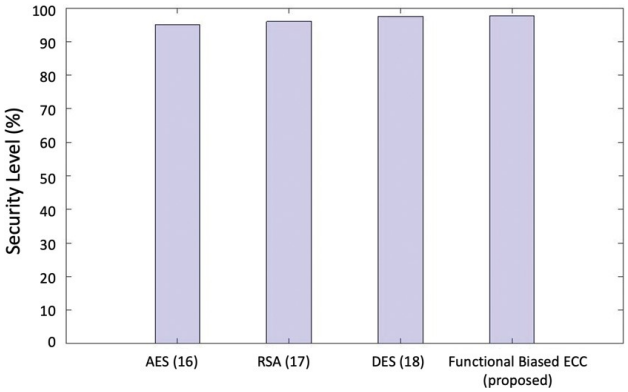

*圖 6.*安全層級分析。AES：進階加密標準、DES：資料加密標準、ECC：橢圓曲線加密法、RSA：Rivest-Shamir-Adleman：Rivest-Shamir-Adleman.

圖 3 至圖 6 說明了 AES、RSA、DES 等 各種演算法與建議方法 FB ECC 在各種參數上的比較：

i) 加密時間

ii) 解密時間

iii) 金鑰生成時間

iv) 安全等級

對演算法的整體分析顯示，在所有討論的四個參數上，它都比傳統演算法提供更好的結果。

結論

為了保護病人的醫療資訊儲存於霧化雲端資料庫，本系統設計了一個安全的醫療資訊儲存模型。醫療資訊來自本系統中支援電子醫療照護小工具的許多病患。

FB-ECC 技術用於部署需要解密和加密以進行通訊的私有伺服器。本研究使用功能性 FB-ECC 方法在受保護的儲存架構上執行加密、解密及金鑰產生程序。與現有的方法比較，建議的技術在安全性、加密、解密和 KGT 方面都優於現有的方法。建議的加密演算法 FB-ECC 的安全等級為 98.64%。有研究顯示，將 FC 與區塊鏈結合，提高了醫療保健的資訊傳輸安全性。由於只有功能偏差的 ECC 密鑰才能傳回實際資訊，因此任何未經授權的個人都無法擷取被隱藏的醫療資訊。

未來在此領域的研究可能包括開發一種新的加密算法，也 就是 FB-ECC 的升級建議加密方式，具有更高的安全性[18]。

經費

本文的編寫過程中未使用任何資金。

利益衝突

沒有利益衝突。

貢獻者

本文由作者負責撰寫。

資料可用性聲明 (DAS)、資料分享、可重複性及資料庫

資料不可用。

應用人工智能產生的文字或相關技術

未使用 AI。

參考文獻

1. Bouachir O, Aloqaily M, Tseng L, Boukerche A. Blockchain and fog computing for cyberphysical systems: the case of smart industry.Computer.https://doi. org/10.1109/MC.2020.2996212
2. Eskandarian A. Scanning the issue.IEEE Trans Intell Transp Syst.2023 Sep 1;24(9):8899-918. https://doi.org/10.1109/TITS.2023.3299370
3. Onasanya A, Elshakankiri M. Smart integrated IoT health-care system for cancer care.2021;27:4297-312. https://doi.org/10.1007/s11276-018-01932-1
4. Ngabo D, Wang D, Iwendi C, Anajemba JH, Ajao LA, Biamba C. Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. 電子。https://doi.org/10.3390/electronics10172110
5. Baniata H, Kertesz A. 區塊鏈-霧整合方法調查.IEEE Access.2020 Jun 1;8:102657-68. https://doi. org/10.1109/ACCESS.2020.2999213
6. Tariq N, Asim M, Al-Obeidat F, Zubair Farooqi M, Baker T, Hammoudeh M, et al. The security of big data in fog-enabled IoT applications including blockchain: a survey.Sensors.2019 Apr 14;19(8):1788. https://doi.org/10.3390/s19081788
7. Banerjee A, Mohanta BK, Panda SS, Jena D, Sobhanayak S. A secure IoT-fog enabled smart decision making system using machine learning for intensive care unit.In: 2020 International Conference on Artificial Intelligence and Signal Processing (AISP).2020 Jan 10 (pp. 1-6).IEEE [於 2024 年 8 月 05 日引用]。Available from: https://www.researchgate.net/publication/340896382_A_Secure_IoT-Fog_Enabled_Smart_Decision_Making_system_using_Machine_Learning_for_Intensive_Care_unit.
8. Fernández-Caramés TM, Froiz-Míguez I, Blanco-Novoa O, Fraga-Lamas P. Enabling the internet of mobile crowdsourc-ing health things: a mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes melli-tus research and care.Sensors.2019 Jul 28;19(15):3319. https://doi.org/10.3390/s19153319
9. Muthanna A, Ateya A, Khakimov A, Gudkova I, Abuarqoub A, Samouylov K, et al. Secure and reliable IoT networks using fog computing with software-defined networking and block-chain.J Sensor Actuator Netw. 2019 Feb 18;8(1):15. https://doi.org/10.3390/jsan8010015
10. Srivastava A, Jain P, Hazela B, Asthana P, Rizvi SW.雲端運算、物聯網和區塊鏈技術在醫療保健產業的應用。在：霧狀運算應用於醫療保健4.0 環境：技術、社會與未來影響。2021:563–91. https://doi.org/10.1007/978-3-030-46197-3_22
11. Yánez W, Mahmud R, Bahsoon R, Zhang Y, Buyya R. Data allocation mechanism for Internet-of-Things systems with blockchain.IEEE Internet Things J. 2020 Feb 10;7(4):3509-22. https://doi.org/10.1109/JIOT.2020.2972776
12. Kumari A, Tanwar S, Tyagi S, Kumar N. Fog computing for Healthcare 4.0 environment: opportunities and challenges.Comput Elect Eng. 2018 Nov 1;72:1-3. https://doi.org/10.1016/j.compeleceng.2018.08.015
13. Pareek K, Tiwari PK, Bhatnagar V. Fog computing in health-care: a review.In IOP Conference Series：材料科學與工程 2021 年 3 月 1 日 (Vol. 1099, No. 1, p. 012025).IOP Publishing.
14. Hanumantharaju R, Pradeep Kumar D, Sowmya BJ, Siddesh GM, Shreenath KN, Srinivasa KG.醫療照護 4.0 中霧運算的啟用技術：挑戰與未來影響。In：醫療保健 4.0 環境的霧計算：技術、社會與未來影響.2021:157-76.
15. Mayer AH, Rodrigues VF, da Costa CA, da Rosa Righi R, Roehrs A, Antunes RS.Fogchain: a fog computing architec-ture integrating blockchain and internet of things for personal health records.IEEE Access.2021 Sep 1;9:122723-37. https://doi.org/10.1109/ACCESS.2021.3109822
16. Munirathinam T, Ganapathy S, Kannan A. Cloud and IoT based privacy preserved e-Healthcare system using secured stor-age algorithm and deep learning.J Intell Fuzzy Syst.https://doi.org/10.3233/JIFS-191490
17. Al Hamid HA, Rahman SM, Hossain MS, Almogren A, Alamri A. A security model for preserving of medical big data in a healthcare cloud using a fog com-puting facility with pairing-based cryptography.IEEE Access.2017 Sep 28;5:22313-28. https://doi.org/10.1109/ ACCESS.2017.2757844
18. Yadav K, Alharbi A, Jain A, Ramadan RA.基於物聯網的安全患者健康監測系統。Comput Mater Contin.2022 Jan 1;70(2):3637-52. https://doi.org/10.32604/cmc.2022.020614