BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

技術摘要與簡報

降低 ZKML 醫療保健應用的模型複雜性：ZKML 應用程式的隱私權保護與推論優化 - 使用合成 ICHOM 資料集的參考實作

Sathya Krishnasamy, MS;[1] 和 Ilangovan Govindarajan, MD[2]

([1]美國康乃狄克州 Newington ChainAim 總裁兼負責人，[2]內華達州拉斯維加斯 GuardianMedx 首席醫療官：Sathya Krishnasamy，電子郵件：sathya.krishnasamy@chainaim.com

DOI: https://doi.org/10.30953/bhty.v7.340

Keywords: blockchain, diabetes, distributed ledger, model complexity reduction privacy, machine learning, ICHOM, International Consortium for Health Outcomes Measurement, ZKML, zero-knowledge machine learning

摘要

Web 3.0 代表著網際網路的下一次重大演進，它體現了底層分散式網路架構、分散式分類帳以及先進的人工智能功能。儘管這些技術正快速成熟，但在大規模採用上仍存在相當大的障礙。作者在 2023 年發表於 Blockchain in Healthcare Today 的一篇名為 Moving Beyond POCs and Pilots 的早期論文中，討論了這些障礙以及透過特定技術的成熟來解決這些問題的緩解措施。這些技術包括隱私保護技術、鏈外和鏈上設計優化，以及規劃和採用這些技術所需的多維方法。作為延伸，本文將討論零知識機器學習 (ZKML)，它以獨特的方式融合了兩種技術流，以解決隱私和推理成本方面的問題。零知識證明 (ZKP) 允許一方向另一方證明某項陳述的有效性，而無需透露該陳述本身的任何額外資訊。ZKML 結合了 ZKP 的加密原理與機器學習 (ML) 技術。它仍是一項日漸成熟的技術，需要基線來應用於全球醫療保健。在這項工作中，作者概念化了使用 ZKML 的技術和操作功能，並在全球醫療照護環境中，針對大量資料收集（包括病患報告的結果）的評估階段，使用合成的國際健康結果測量聯盟 (ICHOM) 實作了參考醫療照護實作。針對 ICHOM 糖尿病資料集研究並報導降低模型複雜度的方法，以推進 ML 模型在全球標準醫療照護資料收集網路分散架構中的使用，從而提高資料保護與效率。

提交：2024 年 8 月 1 日；接受：2024 年 8 月 25 日；發表：2024 年 8 月 31 日

近年來大量的資料收集已產生前所未有的分析能力。然而，隨著資料擷取和機器學習 (ML) 的快速增加，尤其是在集中式系統中，資料隱私和安全性的疑慮隨著過度的資料移動而大幅增加，有時甚至並非真正需要。隨著中央資料庫越來越大，它們也成為了吸引人的目標。醫療照護資料外洩的情況越來越嚴重。常見。已經發生了許多引人注目的事件，而且這種趨勢一直在持續。

降低醫療照護資料相關風險的關鍵策略是在源頭限制資料存取，並減少不必要的資料移動。這包括使用角色存取、資料加密、最小化資料傳輸和定期稽核等方式存取資料。雖然這些都是最重要的，但設計可在分散式網路間溝通的協作系統也很重要。零知邊緣證明 (ZKP) 可以設計為系統之間的證據和驗證，甚至是在區塊鏈之前。這些

附錄

零知識機器學習 (ZKML) 是加密和 ML 技術的革命性融合。

零知識機器學習 (ZKML) 是加密和 ML 技術的革命性融合。它結合了 ZKP 的加密原理與 ML 技術。透過將 ZKP 與 ML 整合，ZKML 可確保敏感資料的機密性，同時仍允許開發和使用預測模型。在資料隱私和安全性極為重要的情況下，例如在醫療保健系統中，這種整合的重要性與日俱增。

實際上，ZKML 允許多個實體進行協作，而不會損害其專有資訊的機密性。這表示組織可以在不暴露資料的情況下，協同在重要資料集上訓練和使用 ML 模型。舉例來說，醫療研究機構可以彙集來自不同醫院的資料，以開發健全的疾病預測模型，而無需任何醫院分享其病患資料。加密證明的使用可確保資料在整個過程中保持安全和隱私。

目前，ZKML 仍處於研究與開發的初期階段。雖然 ZKPs 自 1980 年代起就是加密研究的主題，但其在 ML 上的應用卻是全新且複雜的。這項技術面臨計算效率和資源需求的挑戰。實施 ZKPs 可能是資源密集型的，會增加處理時間和成本。

降低模型複雜度是一種最新的技術，可降低模型複雜度，從而減少計算時間。我們嘗試使用 Kaggle 中較簡單的模型。國際醫療成果衡量聯盟 (International Consortium for Health Outcomes Measurement, ICHOM) 致力於開發標準的成果衡量集，可 在全球使用以評估各種醫療狀況的照護品質。本研究旨在評估全球標準醫療照護資料集（ICHOM）的使用情況，並針對一個真實世界的非瑣碎範例，將模型複雜性降低應用於 ICHOM 模式中的合成資料集。因此，本研究將成為開發更多模型和優化的參考，使其有助於優化 ZKML 的複雜性和使用，以應用於醫療保健領域中需要隱私和協同決策的許多使用個案。

典範轉移：分散式系統、源 AI 模型與協同決策

當我們接近建立在分散式系統上的新興架構時，限制來源資料以及瞭解透過隱私保護的 ML 來處理來源資料的方法變得非常重要。資料是

在美國醫療照護等系統中， 需要有效的機制來啟用聯盟學習、解決隱私與安全問題，並降低計算開銷。透過分享模型更新而非資料，聯合學習可增強隱私。同樣地，對於分散式分類帳，越來越流行的設計概念是透過 ZKP 為驗證系統提供證明。雖然這不是一個新的概念，但這種方法已經成功地擴充了區塊鏈系統，並且在下一代分散式分類帳方面越來越受歡迎。這些機制也能降低資料傳輸風險，並符合資料保護法規及協同決策。ZKML 是一種很有前途的新興技術，它將 AI/ML（人工智慧/機器學習）技術整合到分散式帳本中。

ZKML 對醫療照護隱私權的影響

醫療照護資料相當敏感，因此隱私權是醫療照護系統的首要設計原則。有了 ZKML，醫療照護提供者可以分享從 ML 模型衍生出來的洞察力，而不需揭露底層的病患資料。例如，醫院可以使用 ZKML 模型來預測病患的結果。模型會處理資料並產生預測，而 ZKP 則會確保這些預測的準確性，但不會透露特定的病患資訊。ZKML 允許不同的實體協同計算結果，而不會洩露其個別資料。這在醫療保健研究中特別有用，因為多個機構可能希望結合各自的資料來改善疾病預測，而又不會損害病患的機密性。由於資料隱私權的問題日益嚴重，對安全 ML 模型的需求也與日俱增，因此整合先進的隱私權保護技術變得至關重要。

文獻回顧

ZKPs 是一種加密方法，可讓一方（證明者）說服另一方（驗證者）某項陳述是真實的，而無需透露該陳述本身的有效性以外的任何額外資訊。由 Goldwasser、Micali 和 Rackoff (1985) 提出，[1]他們建立了互動證明和 ZKPs 的理論架構，證明了其可行性和基礎重要性。

Fiat 和 Shamir[2]的進一步工作將其擴展到非互動 ZKP，它不需要證明者和驗證者之間的多輪通訊。最近 ZKPs 的進展，例如 Ben-Sasson 及其同事[3,4]所提出的 Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs)，提升了 ZKPs 的效率與可擴充性，並開啟了實際應用的可能性。

最近，ML 在建模 [醫療保健預測任務] 方面取得了成功，範圍從疾病診斷到醫療保健預測。

引用：Blockchain in Healthcare Today 2024, 7: 340 - https://doi.org/10.30953/bhty.v7.340

病人治療的預後情況。Guerra 及其同事[5] 針對訓練與推論回顧了隱私保護的 ML 文獻，並總結出健康照護資料集是多樣化的，其中一小部分考慮使用獨立的標準資料集來驗證。他們指出聯合式學習的集中式訓練存在風險，並呼籲不同實體之間需要合作，橫跨 ML 科學家、醫療照護從業員、隱私與安全專家等多重角色，他們需要隱私保護機制在分散式帳簿上合作。

作為一項新興技術，ZKML 將 ZKP 應用於隱私的 ML，在確保敏感資料保密的同時，允許開發和利用預測模型來保護隱私和進行協作。因此，ZKP 的計算成本很高，對於 ML 推理證明而言，計算成本會變得更高。最近，Alejandro Martinez Gator[6] 製作了一個模型複雜性減緩器 (MCR) 函式庫，並說明其在多個資料集上的參考實作。然而，從全球醫療照護的角度來看，有必要以高規模的標準化全球醫療照護模式來驗證和基準這項工作。

研究方法

研究目標

Guardian Medx 是一項全面的照護計劃，提供個人化的醫療照護與持續的監測與協助。其目標在於改善印度西南部地區老年人的健康，並減少住院率。主要目的在於遵循評估程序，首先學習印度南部早期在糖尿病照護方面所做的工作[7]，並找出疾病動態中所涉及的文化元素，從診斷、治療、依從到持續維護，並尋找合適的標準化格式，以全面性的基礎擷取臨床和病患報告的結果。其目的在於找到有利於在新興 Web 3 技術中進行隱私保護協作的資料收集模式，包括用於資料分析和隱私保護同意與合作的 ML。

本研究的出發點是尋找一個能解決上述挑戰的高規模標準化全球醫療照護模式，允許充分的資料蒐集，並辨識全球層級協同學習所需的隱私權保護建構。

具體的研究目標包括以下幾點：

- 從早期的研究中學習，並建立一個能捕捉糖尿病照護文化元素的資料收集方法。
- 識別特定的標準化資料模式，該模式可在全球範圍內用於資料收集和隱私權保護學習。
- 探索 ZKML 作為該全球資料模式的模型。
- 使用 MCR 識別參數、限制和緩解措施。
- 以合成資料作為資料模式的基線。

在檢閱有關印度提供糖尿病照護的文獻[7]、大數據收集和 ML 工作[8]，以及標準化格式和適應性報告[9,10]後，決定採用 ICHOM 模式，並進行所需的適應性調整。

ICHOM 資料集與對全球糖尿病醫療照護的影響

ICHOM 致力於開發可在全球使用的標準結果量測套件，以評估各種醫療狀況的照護品質。糖尿病是一種慢性疾病，在不同的文化和醫療照護體系中，其表現和管理都有顯著的差異，因此這種標準化是非常重要的。

糖尿病照護會因文化差異、社會經濟因素和醫療照護基礎結構而有顯著的差異。舉例來說，高收入國家的管理策略和病患結果可能無法直接適用於資源和健康文化態度不同的低收入環境。ICHOM 的資料集可讓醫療照護系統因應當地情況調整標準化的量測方法，以因應這項挑戰。這種文化量身訂做的方式可確保結果指標在不同的環境中都具有相關性和實用性，從而提高資料集的效用和對全球健康結果的影響。

透過提供一套標準的衡量標準，ICHOM 有助於找出不同地區和人口在照護和結果方面的差距。ICHOM 糖尿病資料集採用統一的方法來衡量血糖水平、生活品質和併發症發病率等結果，讓醫療照護提供者能夠根據全球標準來衡量其績效，找出最佳做法，並改善病患照護和人口健康群組。鑑於資料的性質和標準化的努力，主事者以合成資料集開始評估。他們使用 ICHOM 較年長族群和糖尿病資料集來深入瞭解糖尿病照護的複雜性及其對病患結果的影響。

本研究透過收集和分析人口統計、診斷、生活方式和社會因素、治療方法、糖尿病控制、急性事件、慢性併發症和患者報告結果等資料，提供以資料為導向的全面糖尿病管理方法。

結果。它旨在揭示影響糖尿病管理的各種因素之間錯綜複雜的相互影響，並通過早期診斷和規模化的遠端持續監測，以具有成本效益的方式優化糖尿病護理。

作為研究資料評估工作的一部分，研究人員根據早期文獻和經驗製作了具有假設值的合成資料集。使用 ICHOM 糖尿病資料集 V5.0 建立資料充足性、基線和有意義的資料映射，以便在印度文化環境中進行實際部署。這些資料集選自 ICHOM V5 糖尿病資料集。為 100 位病患建立合成資料，並經過多次反覆的資料和臨床驗證。利用單元和雙元分析及關聯分析進行探索性資料分析。

該模型使用 Light Gradient Boost-ing Machine (LightGBM) 回歸器建立，LightGBM 是一個開放源碼、高效能的梯度提升框架，專為高效且可擴充的 ML 任務而設計。它特別針對速度和精確度進行了測試，因此成為不同領域中結構化和非結構化資料的熱門選擇。LightGBM 的主要特點包括：能夠處理數百萬行和數百萬列的大型資料集、支援平行和分散式運算，以及使用基於組織圖的技術和葉向樹生長的最佳化梯度提升演算法。

ZKML 的一個關鍵方面是降低模型複雜性，這對於目前的推理成本和分散式總帳技術的可擴展性來說至關重要，可讓這些模型在真實世界的應用中更有效率、更實用。本文將探討在 ZKML 的情境中降低模型複雜度的概念，並提供具體範例，以及重點介紹其在醫療保健領域中的重要角色。降低模型複雜度的概念包括：修剪 - 移除模型中對最終決策貢獻最小的不必要部分；量化 - 降低權重和啟動的精確度以提高計算效率；以及知識提煉 - 將知識轉移到仍保留預測能力的簡化模型中。這個簡化的模型可以用在 ZKML 架構中，以有效率地執行計算，同時透過 ZKPs 提供隱私權保證。此外，鑑於交叉學習的潛在洞察力，一個延伸目標是確定在證明與驗證系統中有效使用 ZKML 應用所產生的合成資料的技術可行性。而不失隱私。

降低 ICHOM 糖尿病合成資料集的模型複雜度

在 ZKML 中降低模型複雜度對於減緩過度擬合、改善可解釋性並提高計算效率、減少用於訓練和推理的計算資源非常重要。ZKML 軟體及其模型還原函式庫為 GIZA ZK Cook。

複雜度還原演算法執行下列步驟。

1. 相關性分析與特徵重要性，用於特徵選擇與減少：具有高相關性的特徵是可能有助於冗餘和減少的候選特徵。使用遞歸特徵消除等技術，消除重要性低的特徵。
2. L1 (Lasso) 正規化會將不太重要的特徵係數歸零，而 L2 (Ridge) 正規化會懲罰大的係數，以降低複雜性，但不會消除特徵。L1 和 L2 正則化會結合使用，以平衡兩者的優點。對於樹狀模型，修剪會移除對預測貢獻最小的分支，並整合和分割節點。
3. 主成分分析 (PCA) 和 t-distributed Stochastic Neighbor Embedding (t-SNE) 應用於降維。
4. 多通交叉驗證和超參數調整，以平衡模型複雜度和準確度。

使用 Giza 函式庫中的 MCR。分析模型在 Python 環境中執行。

結果與討論

評估階段的資料校正顯示了 ICHOM v5 資料集在定期與持續監測中實際大量使用的可行性，可預防病情惡 化 、降低生活品質（圖 1）、與生活品質評分的關係（圖 2），以及依從性如何細粒度映射（圖 3）。

Guardian Medx 根據匿名萃取的南印度族群早期綜合結果所產生的合成資料進行臨床評估，認為該模型對於推進以結果為基礎且具成本效益的遠端醫療有顯著的幫助。

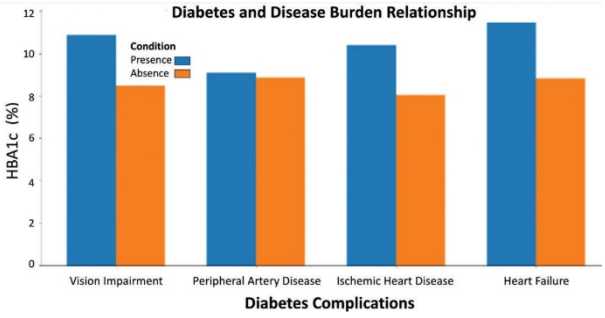
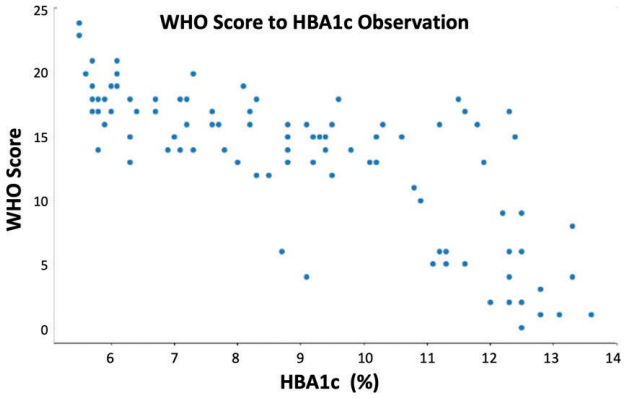


*圖 1.*糖尿病生活品質併發症。HBA1c：糖化血紅素。
資料來源：作者版權所有

引用：Blockchain in Healthcare Today 2024, **7**: 340 - https://doi.org/10.30953/bhty.v7.340

監控照護，基於第一階段分析資料的資料分析和變量



資料來源：作者版權所有

模型。特別是

尤其是在 HBA1c（糖化血紅素）的控制、追蹤頻率、與療效及生活品質評分的關係方面。其他慢性疾病並存的情況在資料中也很明顯。ICHOM 資料捕捉病患報告的結果與 WHO 評分，結果顯示生活品質評分隨著 HBA1C 報告值的增加而呈現負值趨勢。所有依從性指標也顯示出與 HBA1c 結果的預期關係。

這項研究讓我們有可能在遠端監控饋送（feeds）進入大範圍病患管理以進行早期介入時，根據升級預測發出行動警示。

模型還原前的模型複雜性

關鍵在於評估此合成資料集的模型複雜度降低基線，並比較模型複雜度降低基線的結果。

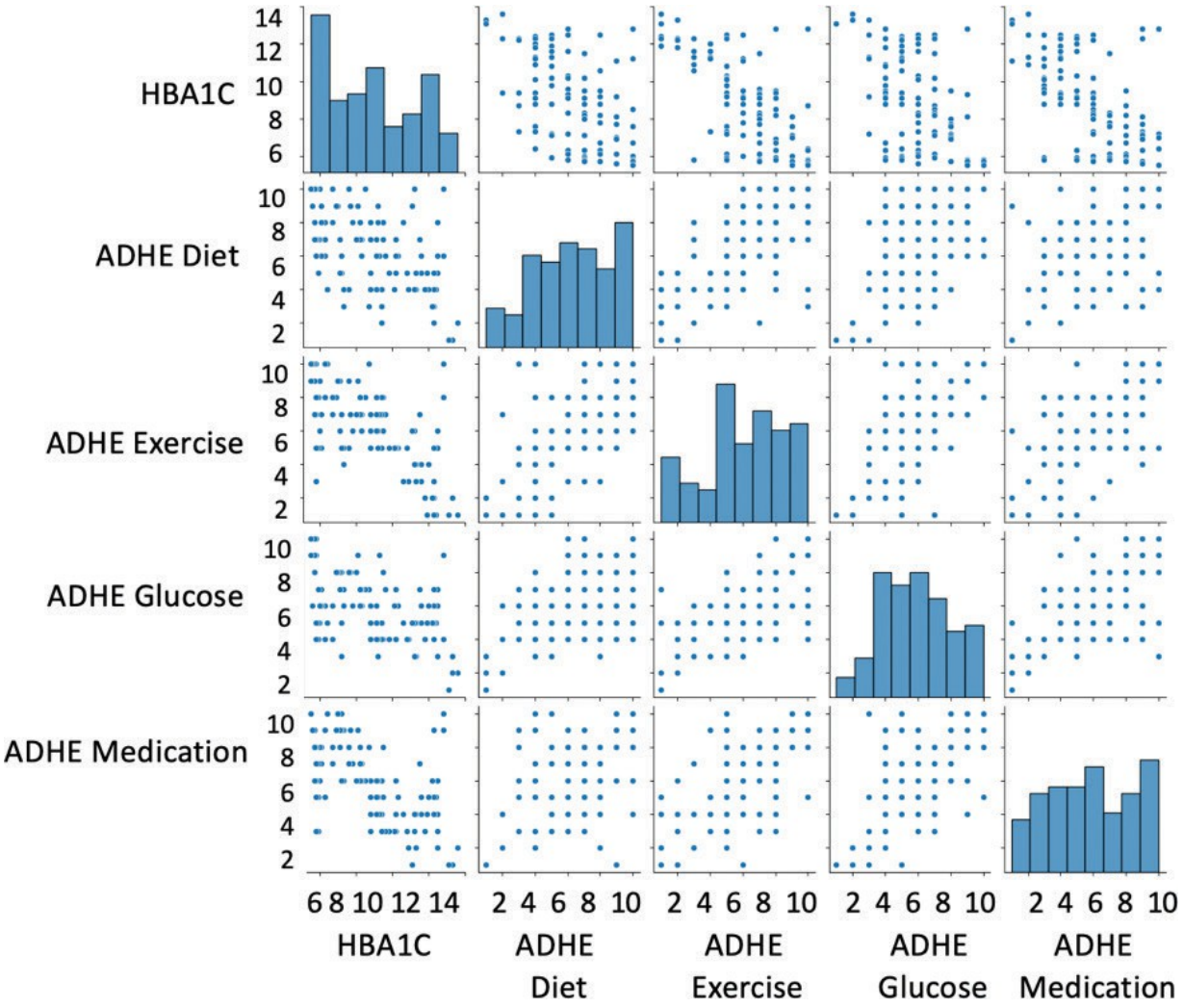


圖 3. 堅持 (ADHE) 對 HBA1c (糖化血紅素) 控制的影響。來源：作者版權所有

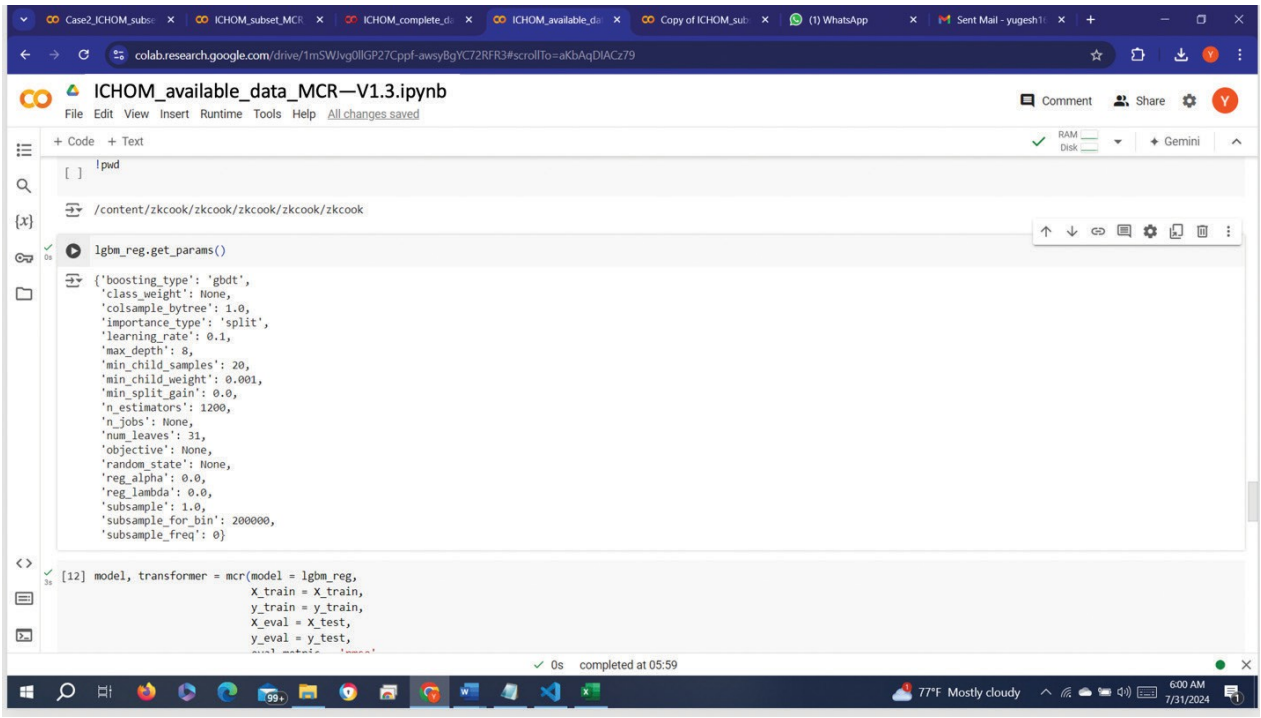


圖 4 降低模型複雜性前的模型複雜性。ICHOM：International Consortium for Health Outcomes Measurement；MCR：model complexity reducer。

來源：作者版權所有：作者擁有版權

模型參數複雜性降低前後的模型複雜性。這對於優化運行時間成本以及了解此模型在分佈式 ML 和分佈式分類帳上的協作系統中的使用情況至關重要。

LGBM 回歸器的參數設定為 n-estimators：1,200 和最大深度：8（圖 4）。相比之下，模型複雜度降低到 n-estimators：150 和 max-depth：4：150 和 max-depth：4，通過 ZKCook 函式庫運行後，模型複雜度降低（圖 5）。

以節點表示：

- 節點數= 樹的數量* (2 ^{深度}-1)
- 複雜性降低前的節點數估算為 1,200 * (2 $^{(8)-1}$) = 306,000
- 複雜性降低前的節點數目為 150 * (2 $^{(4)-1}$) = 2,250

降低模型複雜度後的模型複雜度

這個差異降低了 99.26%，也符合其他一些參考範例。根據評估資料選擇問題的迴歸因子，並使用 MCR 進一步降低複雜度，顯示 ICHOM V5 糖尿病資料集可用於擷取資料，以便增強互操作性，在協作設定中研究和報告結果，以用於 ZKML 應用程式。

這些結果意味著糖尿病研究所需的適應性可以在 ICHOM 的全局 for-mat 中捕捉到，並根據評估資料顯示出前景。此外，這些結果還顯示了為驗證系統生成隱私保護證明的前景，以及以隱私保護的方式與其他合作方協同分享基於患者同意的診斷證明的前景。鑑於評估階段的這些結果，一旦研究取得進展，便可針對計算效率產生最佳化的證明。

這個特定的改編包括了 ICHOM 資料集完整字典的一個子集，因為它是為了這個臨床環境而改編的，這是一個限制。因此，我們將此視為其他工作的起點，將標準化資料集（例如 ICHOM 資料集）用於不同的群組，以及 ICHOM 資料集中的其他疾病。其中有些情況會有更多的資料列數和資料分析需求，這將為我們提供更多的參考點，以了解基線前後的com-plexity 及其對於證明和驗證系統的影響。此外，需要注意的重要一點是，這只是初步的基線，因為技術從各個角度來看都會非常快速地成熟 - 標準開發、模型還原技術、證明的還原，以及驗證系統在軟體和硬體層級上的加速。因此，這將會成為

引用：Blockchain in Healthcare Today 2024, 7: 340 - https://doi.org/10.30953/bhty.v7.340

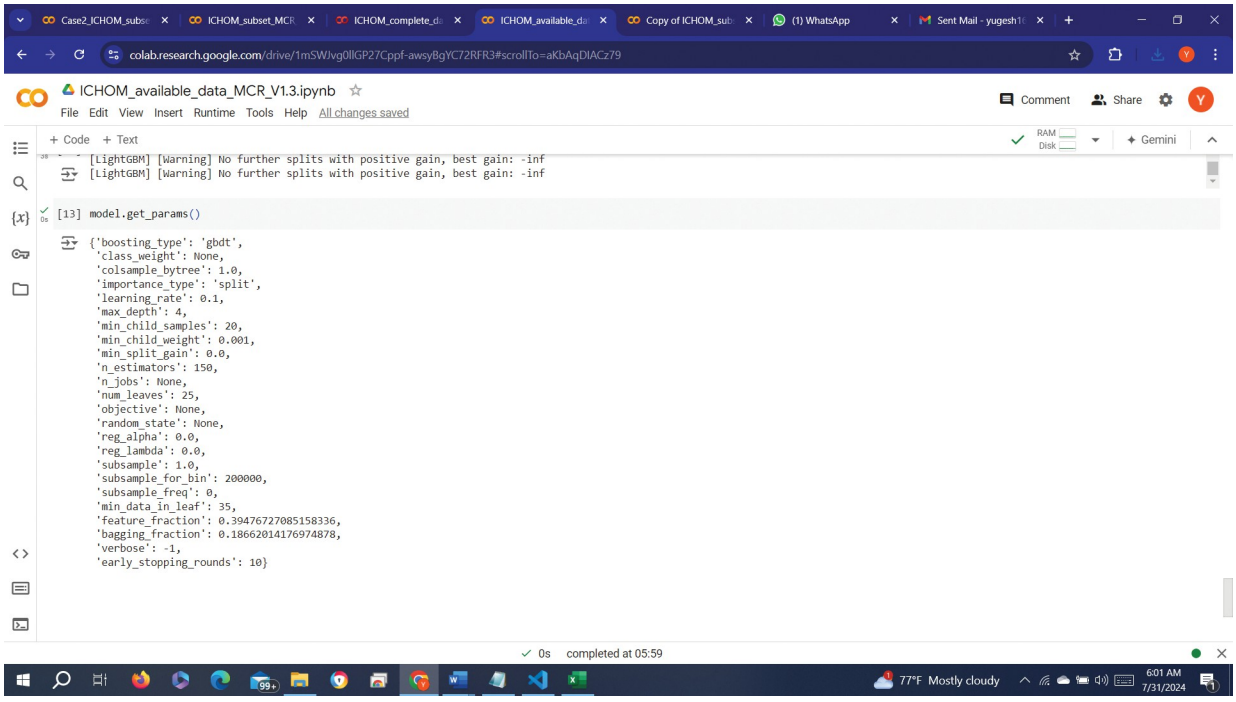


*圖 5.*模型複雜性降低前的模型複雜性。ICHOM: International Consortium for Health Outcomes Measurement；MCR: model complexity reducer。

資料來源：來源：作者版權所有

對於這些參數的 ZKML 發展進行註冊是很重要的。

結論與未來工作

根據評估階段所分析資料的資料分析與迴歸因子模型，GuardianMedx 臨床評估認為該模型有助於大幅推進以結果為基礎且具成本效益的遠端監控照護。將 Giza ZKcook 模型複雜性降低演算法應用於 ICHOM 糖尿病資料，可產生更多可解釋且計算效率更高的模型。在標準化的 ICHOM 資料集上，運算時間大幅縮短，以使用 ML 和隱私保護設定，在源頭保留資料。這可增加安全性，並為任何驅動代理的預測模型提供可驗證的證明，以及在不透露資料內部細節的情況下，將 ML 模型與分散式分散領導者結合使用，以開啟合作的可能性。鑑於評估階段的這些結果，一旦研究取得進展，就可以針對計算效率產生最佳化的證明。進一步的工作可以擴展到 ICHOM 架構的其他調整，在另一個環境中的另一個群組中用於糖尿病，以比較結果，以及在 ICHOM 的其他疾病資料集中使用。不久之後，研究團隊打算將 ZKML 功能擴展至鑽入代理，以進一步處理和推進受隱私保護的多方洞察力。

經費

無。

利益衝突

無。

貢獻者

Sathya Krishnasamy 是 ChainAim Technologies 的總裁兼負責人。他擁有 25 年的專業背景，曾在美國領先的醫療保健公司 (包括 Aetna 和 Anthem) 擔任管理式保健付費者，累積了豐富的經驗。他專注於新興技術，包括 AI/ML 系統和分散式總帳技術。他也擔任許多產業的顧問，包括付款人與醫療服務提供者的合作、標準組織，以及在印度推動金融科技、醫療保健和技能產業的 Account Aggregators 等工作。他目前是 ChainAim 的總裁兼主管，提供技術策略諮詢、應用程式與開發服務。

Sathya Krishnasamy 協助構思 ICHOM 的資料使用、評估合成資料集、建立模型複雜性基線，以及評估 ZKML 醫療保健使用個案。

Govindarajan 博士是 GuardianMedX 的首席醫療官。Govindarajan 博士是 GuardianMedX 的首席醫療官，他是一位

擁有深厚醫學背景和尖端技術的醫療主管。他擁有 35 年豐富

的內部

引用：Blockchain in Healthcare Today 2024, **7**: 340 - https://doi.org/10.30953/bhty.v7.340

他是印度醫學和老年醫學的專家，並擔任印度許多政府單位的老年醫學和緩和療護的顧問。他曾在診所、醫院、療養院、安寧療護中心和家庭中，依照獨特的連續照護方式，管理並執行以病患為中心的優質照護。

Govindarajan 博士發起這項計畫，並進行資料收集需求的研究、糖尿病資料 ICHOM 的設計與評估，以及合成資料集的臨床評估。

資料可用性聲明 (DAS)、資料分享、可重複性及資料庫

ICHOM V5 糖尿病資料字典的資料字典可在 https://www.ichom.org/ patient-centered-outcome-measure/diabetes/ 上取得。

應用 AI 產生的文字或相關技術

無。

鳴謝

Yugesh Panta 是紐約大學 Tandon 工程學院電機與電腦工程系的理學碩士學生，他在研究資料蒐集、驗證、分析和模型調整等方面協助主事者。

參考文獻

1. Goldwasser S, Micali S, Rackoff C. 交互式證明系統的知識複雜性。第十七屆 ACM 計算理論年度研討會-STOC '85。1985.
2. Fiat A, Shamir A. How to prove yourself: practical solutions to identification and signature problems.加密技術進展-CRYPTO' 86 [網際網路].2019;186-94.Available from: https://link.springer.com/chapter/10.1007%2F3-540-47721-7_12 [cited 2024 July 31].
3. Ben-Sasson E, Chiesa A, Tromer E, Virza M. Succinct non-interactive zero knowledge for a von neumann archi-tecture [Internet].2019.Available from: https://eprint.iacr. org/2013/879.pdf [cited 2024 July 31].
4. Ben-Sasson E, Bentov I, Horesh Y, Riabzev M. Scalable, transpar-ent, and postquantum secure computational integrity [Internet]. ePrint IACR.2018.Available from: https://eprint.iacr.org/2018/046 [cited 2024 July 31].
5. Guerra-Manzanares A, Lechuga J, Maniatakos M, Shamout FE.醫療保健的隱私保護機器學習：開放的挑戰與未來展望。ArXiv.2023; 1-13. https://arxiv.org/abs/2303.15563
6. Gotor AM.最大化模型效率與模型-com-複雜性-reducer (MCR)。zkcook/docs/mcr.pdf at main giza-techxyz/zkcook [Internet].GitHub。[cited 2024 Aug 1].網址：https://github.com/gizatechxyz/zkcook/blob/main/docs/mcr.pdf
7. Das AK, Saboo B, Maheshwari A, Nair VM, Banerjee S, Jay-akumar C, et al. Health care delivery model in India with rele-vance to diabetes care. Heliyon.Heliyon.https:// doi.org/10.1016/j.heliyon.2022.e10904
8. Musacchio N, Giancaterini A, Guaita G, Ozzello A, Pellegrini MA, Ponzani P, et al. Artificial intelligence and big data in diabetes care: a position statement of the Italian Associa-tion of Medical Diabetologists.J Med Internet Res. 2020 Jun 22;22(6):e16922. https://doi.org/10.2196/16922
9. 糖尿病 [網際網路]。ICHOM.[cited 2024 Aug 1].網址：https://www.ichom.org/patient-centered-outcome-measure/ diabetes/
10. Benning L, Das-Gupta Z, Fialho LS, Wissig S, Tapela N, Gaunt S.平衡適應性與標準化：從 27 個常規實施的 ICHOM 標準集中得到的啟示。BMC Health Serv Res. 2022 Nov 28;22(1):1424. https://doi.org/10.1186/ s12913-022-08694-9

附錄

縮寫詞定義

AI/ML：人工智慧/機器學習 HBA1c：糖化血紅素

ICHOM：國際健康結果測量聯盟

LightGBM：光梯度提升機 MCR：模型複雜性降低器

ML：機器學習

zk-SNARKs：Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge（零知識簡潔非互動知識論證

ZKML：零知識機器學習 ZKP：零知識證明