
應用新穎聯邦學習技術於
即時防災預警系統
Applying Innovative Federated Learning
Technology to Real-Time Disaster Warning Systems
(期末成果報告書)

執行單位：國立成功大學

執行期間：113 年 2 月 7 日至 113 年 12 月 31 日

計畫主持人：蔡文柄 助理教授

農業部農村發展及水土保持署 編印

中華民國 113 年 12 月

(本報告書內容及建議純屬執行單位意見，僅供本署施政參考)

應用新穎聯邦學習技術於即時防災預警系統

摘要

崩塌發生時長較短，帶來的損害卻極大，因此預測區域崩塌發生可能性極需被重視；台灣地理位置處於板塊交界處，地震發生頻繁，屬於環太平洋地震帶的一部分，岩層受到地震影響產生擠壓，加上風化作用的影響，導致台灣地質構造脆弱，台灣山區範圍廣大且地形陡峭，加上位處於緯度較低區域，夏秋兩季容易有颱風侵襲，造成短時間且高強度的降雨，水流侵蝕與淘刷現象嚴重，使得台灣山區成為易發生崩塌災害之區域；過去崩塌研究大部分僅是利用收集到的潛勢因子進行不同的崩塌辨識模型建置，或僅直接使用衛星影像跟攝影機的影像資料進行影像辨識，少有將多種異質資料整合之研究；本計畫將蒐集地面氣象資料、崩塌資料、數值高程資料與衛星影像資料，應用人工智慧技術(機器學習、深度學習)及發展完善之軟體，整合前述蒐集之多種異質資料，並嘗試納入先進的聯邦學習方法(Federated Learning)建立多尺度之區域性崩塌潛勢預警系統，同時藉由新穎之深度模型架構特性，模型輸入項限制性小(輸入項彈性)、模型運算時間短、快速即時更新預測模型，建立更加準確的崩塌潛勢預測模型，提早研擬更加有效的撤離政策，減少生命及財產的損失。

關鍵詞：人工智慧技術、機器學習、深度學習、聯邦學習、崩塌潛

勢預警系統

Applying Innovative Federated Learning Technology to Real-Time Disaster Warning Systems

Abstract

Landslides occur over a short duration but can cause significant damage. Therefore, predicting the likelihood of regional landslides is crucial. Taiwan is located at the junction of tectonic plates, making it prone to frequent earthquakes. As part of the Pacific Ring of Fire, Taiwan's rock layers are subjected to pressure from seismic activity and weathering, resulting in fragile geological structures. The mountainous areas of Taiwan are extensive and steep, and the low latitude makes it susceptible to typhoons during the summer and autumn seasons, causing short-term, high-intensity rainfall. Severe water erosion and scouring make the mountainous regions prone to landslides.

Previous landslide research mainly focused on using collected potential factors to build different landslide identification models or directly using satellite and camera imagery for image recognition, with few studies integrating multiple heterogeneous data sources. This project will collect ground meteorological data, landslide data, digital elevation models, and satellite imagery. We aim to integrate these diverse data sources using artificial intelligence techniques (machine learning, deep learning) and well-developed software. This project will also attempt to incorporate advanced federated learning methods to establish a multi-scale regional landslide potential early warning system. By leveraging the novel characteristics of deep model architectures, we aim to create a more

accurate landslide potential prediction model with less restrictive input requirements, shorter computation times, and rapid real-time model updates. This will enable the development of more effective evacuation policies in advance, reducing loss of life and property.

Keywords: Artificial Intelligence Techniques, Machine Learning, Deep Learning, Federated Learning, Landslide Potential Early Warning System

目次

摘要.....	I
Abstract.....	III
目次.....	V
圖次.....	VII
表次.....	VII
第一章 緒論	1-1
第一節 研究目的	1-1
第二節 文獻回顧	1-1
第三節 研究架構	1-3
第二章 工作執行方法與步驟	2-1
第一節 工作執行方法	2-1
第二節 工作執行步驟	2-10
第三章 工作進度與交付項目	3-1
第一節 計畫甘特圖	3-1
第二節 計畫交付項目	3-2
第四章 結論及建議	4-1
第一節 結論	4-1
第二節 建議	4-2
參考文獻.....	參-1
附錄.....	附錄-1

圖次

圖 1、研究流程圖	1-6
圖 2、崩塌區域圖層	2-2
圖 3、ANN 簡易模型示意圖	2-4
圖 4、CNN 架構圖	2-6
圖 5、活化函數示意圖	2-7
圖 6、研究區域客戶端網格圖	2-11
圖 7、客戶端目標區域坡度圖	2-13
圖 8、客戶端目標區域坡向圖	2-13
圖 9、客戶端目標區域雨量點位圖	2-14
圖 10、聯邦學習架構圖	2-22
圖 11、本計畫甘特圖	3-1
圖 12、聯邦學習 1~5 回合迴歸結果圖	3-4
圖 13、聯邦學習 6~10 回合迴歸結果圖	3-6
圖 14、聯邦學習 61~65 回合迴歸結果圖	3-8
圖 15、聯邦學習 1~5 回合分類結果圖	3-10
圖 16、聯邦學習 6~10 回合分類結果圖	3-12
圖 17、聯邦學習 47~52 回合分類結果圖	3-14
圖 18、ROC 及 AUC 結果圖	3-16
圖 19、聯邦學習 1~5 回合 CNN 迴歸結果圖	3-17
圖 20、ANN、CNN 模型 49~50 回合結果比較圖	3-18

表次

表 1、各客戶端與測試區資料表.....	2-15
表 2、混淆矩陣表	2-25
表 3、CNN 回歸結果統計指標表.....	3-18

第一章 緒論

第一節 研究目的

全球受到氣候變遷影響，極端水文事件頻傳，洪水在各國肆虐，自然災害對於人民性命與財產造成重大的威脅，因此災害的風險管理成為不可或缺的重要步驟。臺灣受到地理位置關係影響，夏、秋兩季時常有颱風侵襲，再加上位處板塊交界處，地震發生頻繁且地質脆弱，中央山脈導致臺灣山區坡度較大，在面對強降雨時山區土壤含水量過高，使得台灣成為容易產生山崩或地滑等崩塌現象之區域。

崩塌現象發生的時間極為快速，一旦發生很容易帶來極大的損害，因此預測崩塌發生可能性是極為需要被重視的議題。導致崩塌的原因十分複雜，可能因為坡度、地質條件、土壤含水量或降雨量等因素，加上近年來山坡地開發及砍伐樹林等問題也成為間接導致崩塌發生的原因。過去崩塌相關的研究主要採用定性法與定量法兩大方法，通過蒐集到的潛勢因子進行模型建置或者使用影像資料進行影像辨識，在進行崩塌潛勢分析時容易受到資料的限制，因此本研究嘗試使用新型的人工智慧建立模型，通過神經網路模型學習資料特性，將不同型態之資料放入不同模型運算，進行崩塌判斷，減少需要人力取得參數的問題並讓模型可以通過及時回傳之參數進行即時更新。

第二節 文獻回顧

崩塌(landslide)為邊坡材料因受到重力作用，發生向下滑動或崩落之塊體運動現象(行政院農業委員會水土保持局，2005)。

過去研究中，主要將崩塌相關研究分為定性法及定量法兩種，定量法中包含統計分析及人工智慧方法；統計分析中，有研究利用降雨量對崩塌地區進行分析，採用多變量分析的羅吉斯迴歸建立山崩潛勢模式，找出崩塌與降雨之關係，並對具有致災規模之崩塌進行警戒(中興工程顧問社，2018)。而在人工智慧方面，近年來也有研究利用人工類神經網路建立崩塌比率評估模型，可以有減少人工求取參數、快速得到回傳的數據進行運算等優勢(李秉乾等人,2019)。

人工智慧(Artificial intelligence, AI)快速發展，藉由 ChatGPT 被廣為人知，各種不同方法的模型蓬勃發展。利用模擬人類大腦神經網路系統而架構的人工神經網路(Artificial Neural Network, ANN)，在 1989 年被成功用來辨識手寫字體(LeCun et al., 1989)，此後，越來越多隱藏層被成功開發，提高預測的準確度，也被應用在更多的領域上，例如：語音識別、語言翻譯及醫學診斷等。隨著不同種類的模型被開發，模型被分為監督式學習與非監督式學習，通過人工進行標籤的方式，用大量被標籤的資料對未知資料進行訓練，這種方法稱為「監督式學習」，而事先不對資料進行標注，通過模型學習資料的特性來進行則被稱為「非監督式學習」。根據取得資料型態的差異，也可以選擇不同的模型進行訓練，如果資料為影像，可以使用卷積神經網路(Convolutional Neural Networks, CNN)例如進行：手寫辨識(Li et al., 2015)或者通過 YOLO 進行影像辨識等方法。當資料為數值時，可以根據時序資料採用長短期記憶模型(Long Short-Term Memory, LSTM)進行訓練。

聯邦學習(Federated Learning, FL)為一種協作式去中心化的隱私保存技術，旨在克服數據孤立和敏感數據的挑戰。隨著儲存容量和處理能力的發展，在工業工程中的數據科學的重要性變得更加明顯，但也萌生出了數據孤島問題，此外，在某些領域如醫療行業，數據標註依賴於有經驗的工作者，這可能導致有效數據稀缺，標記數據的稀缺對工業發展也是有害的，而聯邦學習的出現有效的解決了以上的問題(Li, Li, et al., 2020)。Rieke 和 Nicola 等學者於 2020 年提出未來健康數據預測，可由聯邦學習的方式解決資料分布在各個醫院無法取用之現況。Nguyen 等學者於 2021 年探索並分析了 FL 實現各種 IoT 服務的潛力，包括 IoT 數據共享、數據卸載和緩存、攻擊檢測、定位、行動群體感知、以及 IoT 的隱私和安全性，然後，對 FL 在智慧醫療、智慧交通、無人機、智慧城市和智慧工業等各種關鍵 IoT 應用中的使用進行了全面調查。

第三節 研究架構

(一)資料蒐集

本研究以 2021 年發生的崩塌事件為基礎，並結合研究區域的地形數據，包括坡度、坡向與降雨量等重要環境因子。這些數據來源於公開的地質調查資料庫和氣象觀測數據，為山崩預測提供了豐富的特徵信息。蒐集後的數據會依據空間分布劃分成多個子區域，以便模型能針對各區域進行針對性的分析和預測。

(二)資料整理

在資料整理階段，為了提升數據的利用價值並方便模型訓練，輸入數據經過網格化處理，將研究區域分割成大小一致的網格單位。每個網格單位內的坡度、坡向、降雨量等特徵經過統計處理，以代表該網格的整體特性。為了確保資料品質，進一步清理並移除異常值，並標記每個網格單位是否發生過崩塌，以便後續的分類預測。

(三)客戶端模型建置

在每個客戶端模型中，本研究採用了神經網絡結構來處理網格化數據，針對每一網格的特徵找尋輸入與輸出的映射關係。每個客戶端獨立訓練自己地區的數據，以保護各地區數據隱私，並透過自訂損失函數 BME Entropy Loss 提升模型在不平衡資料上的學習效果。

(四)聯邦學習架構設置

聯邦學習架構在中央伺服器上實現，各客戶端的模型會定期將訓練後的參數上傳到中央伺服器。伺服器透過加權平均法聚合這些參數，並在中央驗證集上評估模型性能，確認其預測準確度。此過程不斷迭代進行，直到中央模型的預測效果趨於穩定。透過聯邦學習的設計，將能有效降低需要傳輸原始資料的時間，並提升模型的跨地區泛化能力。

(五)防災預警系統

最終融合的模式整合至防災預警系統中，用以即時分析網格單位的崩塌風險。該系統每隔一定時間更新氣象和地質資料，並將資料輸入至模型以生成各網格的崩塌可能性。當系統檢測到任一網格單位的風險超出預警閾值時，會自動通知相關單位進行應對。此防

災預警系統能提前提供準確的風險評估，協助政府與防災單位及早準備，減少崩塌帶來的危害。

簡言之，防災預警系統的建構方法是先在各地區建立邊緣模型 (Edge Model)。在多個邊緣模型訓練完成後，透過聯邦學習框架整合各模型的訊息，建立輸入資料與崩塌事件之間的映射關係。這種方法避免了中央模型過度依賴特定區域的數據，從而提升模型的廣泛適用性與準確性。利用聯邦學習的高效能特性，可為防災預警系統提供更為穩健的支持。

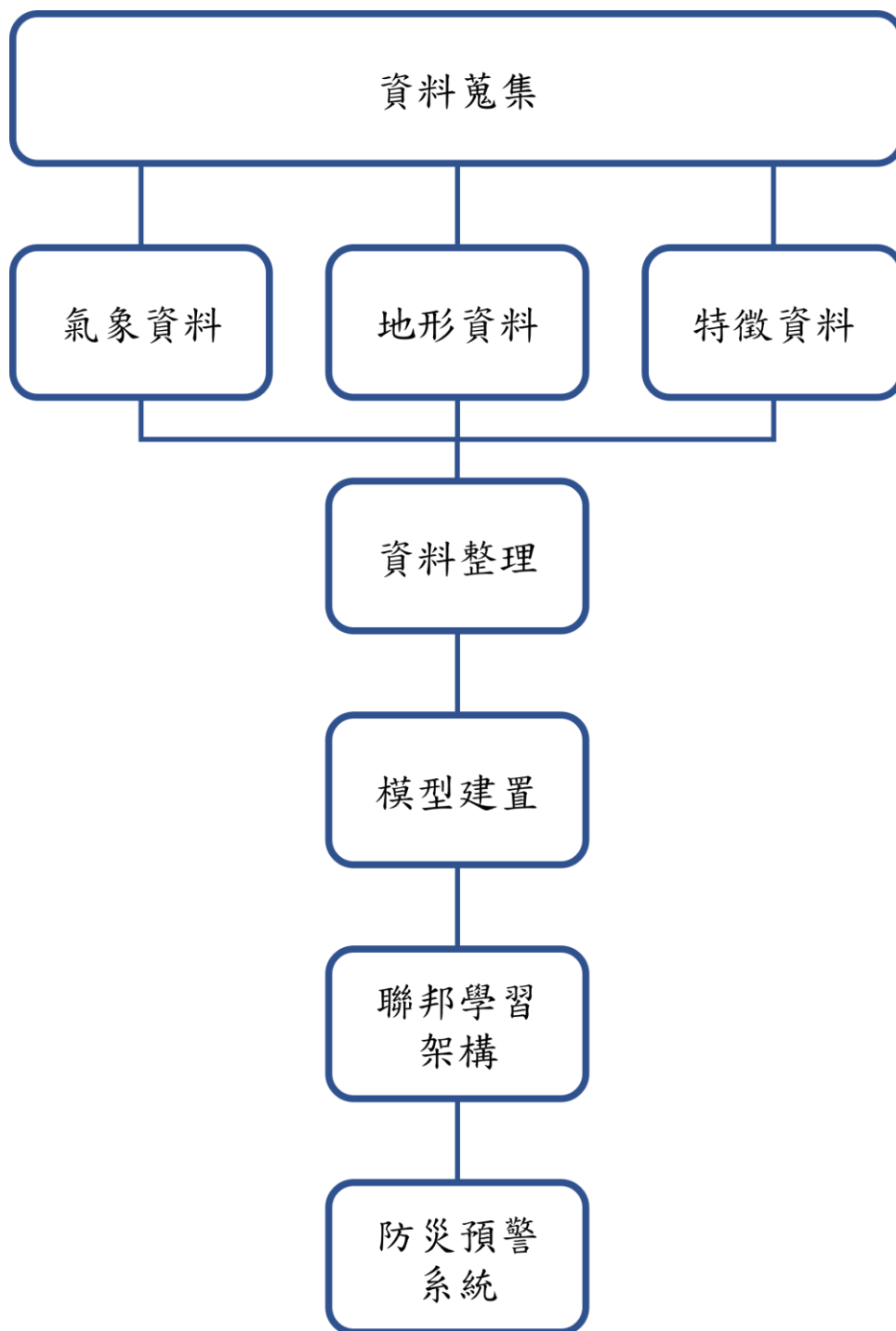


圖 1、研究流程圖

第二章 工作執行方法與步驟

第一節 工作執行方法

一、研究區域

本研究針對崩塌事件進行分析，考量到崩塌資料除衛星影像外，其餘數據多集中於某些特定的年月，缺乏長期而全面的時空覆蓋，因此，本計畫選定崩塌事件較為集中的 111 年 6 月 23 日為研究範本，利用該次事件中豐富的崩塌資料作為分析依據。此事件的崩塌區域涵蓋範圍廣泛，集中在台灣的中央山脈以及茂林區、霧台鄉、延平鄉與南橫公路地區等地，構成該地區崩塌的高危險區域。本研究中的中央模型則採用南橫公路天池至向陽路段區域的資料進行測試，此路段為連接台灣南部區域與花東地區的重要交通幹道，其崩塌風險對交通通行及區域安全影響深遠，具備重要研究意涵。

二、模型資料蒐集

(一)、崩塌(Landslide)

目標崩塌資料來自農村發展及水土保持署資料管理平台(<https://data.ardswc.gov.tw/Map/MapDataIndex>)，透過下載 111 年度全台崩塌地圖層，獲得了包含全台各地崩塌事件的地圖層，作為本研究的預測資料來源。根據該年度的數據分析，中央山脈區

域以及南橫公路路段在 111 年 6 月 23 日發生了密集的崩塌事件，這些事件在空間分布上形成了具有高度風險的區域，鑑此，本計畫選取該日期的崩塌事件作為目標事件，並將此資料用於模型的訓練與預測分析，以期能更準確地模擬崩塌發生的潛在因子及空間分布模式。

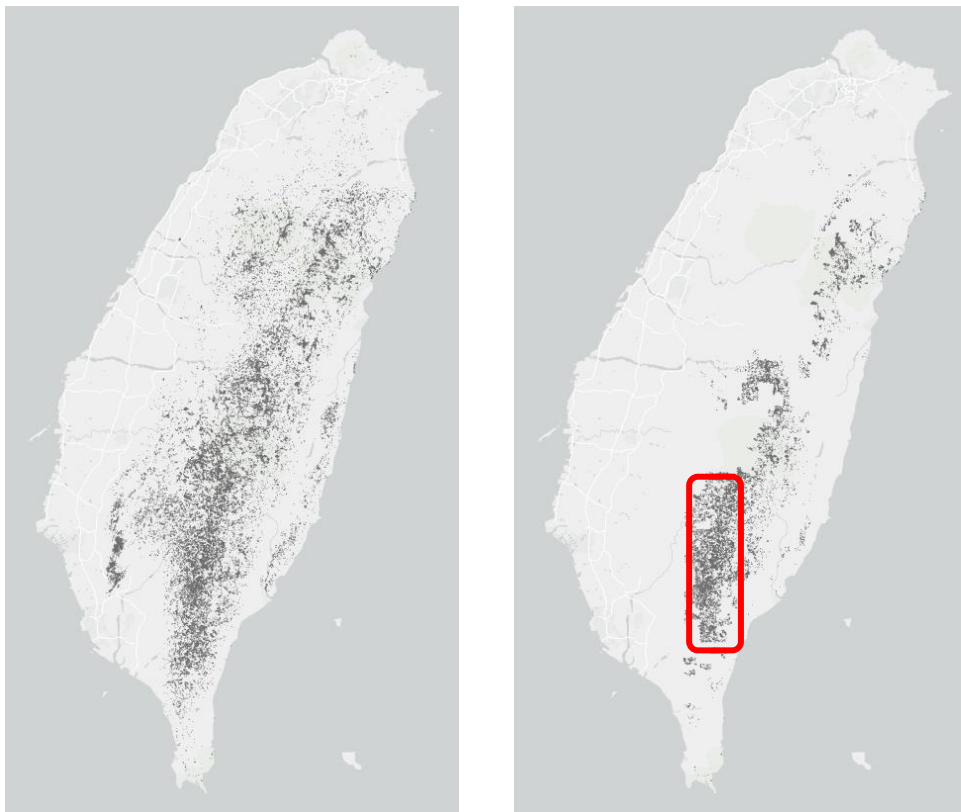


圖 2、崩塌區域圖層

(二)、數值高程地圖(Digital Elevation Map, DEM)

數值高程地圖由政府資料開放平台(<https://data.gov.tw/dataset/35430>)，下載內政部 20 公尺網格數值地形模型資料，取用不分幅之全台及澎湖 DEM 資料。

(三)、雨量資料

雨量資料由臺灣氣候變遷推估資訊與調適知識平台(TCCIP) (<https://tccip.ncdr.nat.gov.tw/index.aspx>) 取得花蓮縣、南投縣、高雄市、台南市、屏東縣及台東縣網格化觀測降雨量日資料，時間跨度由 1960 年 1 月 1 日至 2022 年 12 月 31 日，其網格大小為 0.01° (約 1 公里)。

(四)、類神經網路(Artificial Neural Network, ANN)

人工神經網路 (ANN) 主要模仿生物神經網路的工作原理，用於處理分類、回歸等多種問題。其結構包括多層神經元(neurons)，由輸入層、隱藏層及輸出層所組成，每層神經元與其他層的神經元相互連接，形成網路結構。

在 ANN 中，輸入層接收原始數據，每個輸入特徵對應到一個神經元，這些特徵值會傳送到隱藏層。隱藏層由多個神經元構成，每個神經元接收輸入層的加權輸入，並經由活化函數(activation function) 轉換成非線性輸出，使網路具備學習複雜特徵的能力。常用的活化函數有 ReLU (Rectified Linear Unit)、Sigmoid 和 Tanh 等。本計畫在輸入層及各隱藏層之間使用 ReLU 作為活化函數，輸出層為因應輸出標籤為 2 元分類，所使用的函

數為 Sigmoid 函數，後續會更深入說明。

每層神經元之間的連接帶有權重 (weight)，這些權重會隨著網路的學習過程不斷調整，以最小化輸出結果與實際標籤的誤差。隱藏層處理後的數據傳遞至輸出層，並經過激活函數後得到分類或回歸結果。訓練過程中使用反向傳播 (backpropagation) 方法計算誤差梯度，並藉由梯度下降法 (gradient descent) 或其他優化方法更新權重，進而提高預測準確性。

這種模型結構的優點在於其靈活性和可塑性，適用於數據標籤已知的情況下進行監督式學習，並可以通過多層隱藏層來處理更高維度和更複雜的數據特徵，從而獲得精確的分類結果。

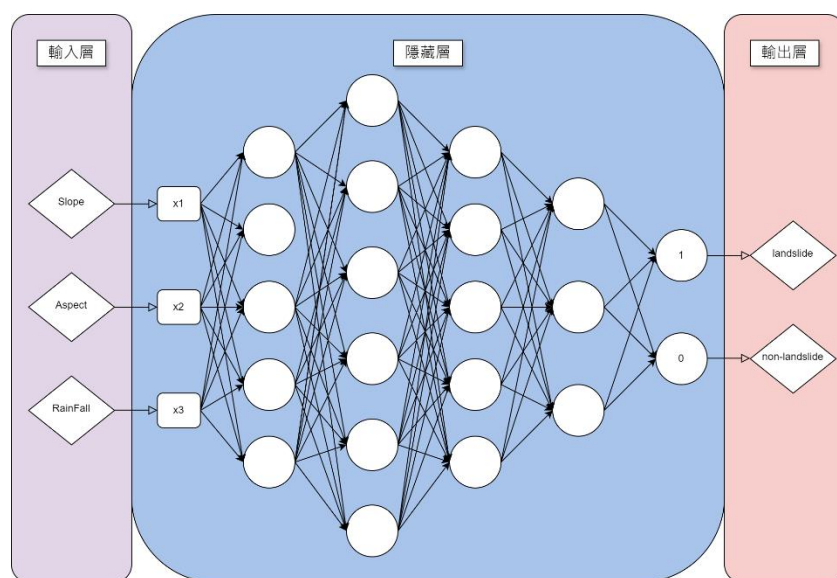


圖 3、ANN 簡易模型示意圖

(四)、卷積神經網路(Convolutional Neural Network, CNN)

卷積神經網路(CNN)常用於辨識圖像資料特徵，藉以處理分類問題，例如：在圖片中若辨識到鼻子、牙齒、耳朵、四肢爪子及尾巴，便將其分類為狗，其中鼻子、牙齒等特徵即為模型辨識出該圖片特徵結果，狗為其分類結果，透過此種方法將已標籤好的資料輸入 CNN 模型使其學習，得到正確的分類結果，此模型結構包含卷積層(Convolution Layer)與池化層(Pooling Layer)：

卷積層：用程式演算法產生一特定大小之卷積核(Convolution kernel)，藉由設定好之移動步伐(stride)在原始圖片上進行逐步掃描，為了使原始資料大小不因為卷積過程一次變得過小，所以使用填充資料(zero padding)在原始外圈上下左右各加 n 行 n 列之 0 值資料，接著進行卷積運算(相乘、加總)，得到特徵地圖(feature map)。

池化層：池化層目的為特徵萃取，也就是將原始圖片資料量減少並保留重要資訊，最常見的方法即為最大池化法(max pooling)，找出特徵地圖中的矩陣內資料的最大值進行映射(mapping)，其餘亦有平均池化法、最小化池化法等。

以上述之卷積層與池化層進行卷積處理後輸入全連接層(fully connected layer)進行結果平坦化，並連接到基本的神經網路執行其他必要之分類運算，此過程為 flattening。下圖為 CNN 模型輸入至輸

出示意流程圖。

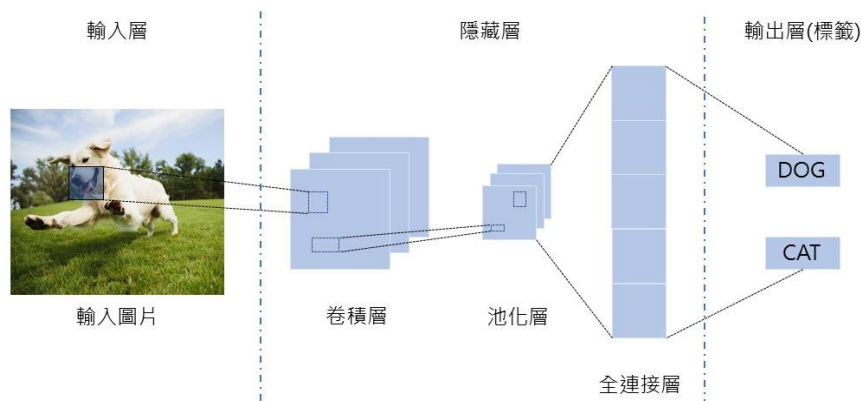


圖 4、CNN 架構圖

(五)、活化函數

當資料輸入模型後，經過每一個隱藏層神經元，均需活化函數將其從神經元輸出，因為類神經網路在訓練時，會以線性的模式進行求解，但實際的問題經常為非線性的，為了減少線性程度，使得類神經網路的分析結果可更準確，活化函數便應用於此以增加類神經網路訓練時的非線性程度，而通過挑選正確的活化函數，才能使模型輸出目標需求的結果。常見的活化函數有 ReLU、Sigmoid 及 Softmax 函數。

ReLU(Rectified Linear Unit)函數：

數學定義為 $f(x) = \max(0, x)$ ，若輸出值為正值，該輸出值經過 ReLU 函數轉換仍為正常輸出，若輸出值為負值，則經過 ReLU 函數轉換後，輸出值為 0。

Sigmoid 函數：

數學定義為 $f(x) = \frac{1}{1+e^{-x}}$ ，常適用於二元分類 (Binary Classification)，其具有非線性且梯度平穩的特性，但當輸入值有離群值時，經過 Sigmoid 函數輸出並不能反映出該值是否為離群值。

Softmax 函數：

數學定義為 $\sigma(x)_j = \frac{e^{z_j}}{\sum_{k=1}^K e^{z_k}}$ ，常適用於多元分類問題，在計算各種類別發生的機率分布時，機率總和為 1，但若離群值存在，會導致結果更加偏離。

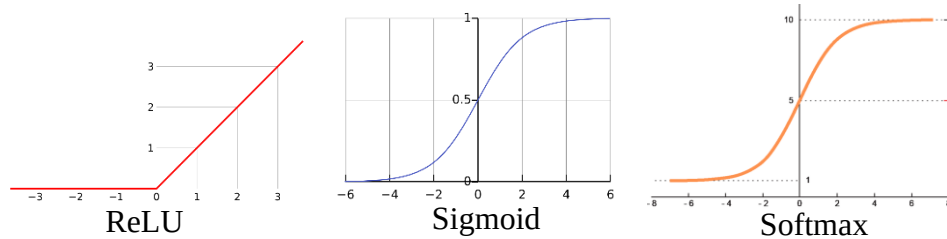


圖 5、活化函數示意圖

(六)、聯邦學習：

聯邦學習 (Federated Learning) 是一種分散式學習 (Distributed Learning) 技術，其核心特點是將資料保存在各個客戶端裝置上，並利用這些裝置的平行運算能力來加速模型的訓練過程。在聯邦學習架構中，數據不需集中於中央伺服器，而是透過各個運算單元的獨立運算來實現模型的優化，進而保護用戶的數據隱私，同時降低數據傳輸的需求。這一分散式設計使得雲端中央模型不會干涉各客

戶端模型的訓練過程及訓練時間，實現了高度的去中心化。

聯邦學習具有多項優勢。首先，其去中心化的架構解決了數據結構和客戶端模型的異質性問題。由於不同客戶端的數據集分佈和模型設定可能各異，聯邦學習允許各個運算單元根據自身的資料特徵進行局部模型訓練，而僅將經過處理的權重或梯度傳回中央進行匯總，進一步減少了數據的傳輸風險與隱私洩露的可能性。

聯邦學習通常包含以下四個步驟：

架構確立 (Formulate Topology)：首先制定聯邦學習系統的拓撲架構，這包括了溝通的順序、資訊流的方向，以及模型在中央伺服器或特定節點進行聚合的方式。拓撲架構確定了每個邊緣端模型如何參與訓練過程，以及資訊如何在系統內部流通。

梯度計算 (Gradient Compute)：各個客戶端會根據其局部數據集 (local dataset) 進行模型訓練，計算出相應的梯度。由於每個節點所擁有的資料可能非獨立且不相同 (Non-IID)，因此這一步的計算會針對各個數據集的特性進行優化，以獲得適合局部數據的模型參數更新。

資訊交換 (Information Exchange)：當每個客戶端完成梯度計算後，會依據設定的拓撲架構來傳送所計算的梯度或模型參數至中央伺服器或其他節點。這一步的資料傳遞方式通常受到隱私

及效率需求的影響，可能採用安全傳輸協議或加密技術，以確保數據在交換過程中的隱私性與完整性。

模型聚合 (Model Aggregation)：中央伺服器會收集所有客戶端傳回的權重或梯度，並使用聚合演算法（例如 FedAvg）對這些更新進行整合。由於不同客戶端的資料通常是 Non-IID 資料，聚合演算法的設計需特別謹慎，以便平衡不同客戶端的貢獻，並有效地優化中央模型。完成聚合後，更新後的模型會同步回各客戶端，以進行下一輪的迭代訓練。

透過上述的迭代過程，聯邦學習能逐步提升模型的準確性，同時滿足數據隱私、分散計算及 Non-IID 數據處理等需求，廣泛應用於金融、醫療等對隱私保護有嚴格要求的領域。

FedAvg 演算法：

FedAvg (Federated Averaging) 演算法是聯邦學習中最具代表性的權重聚合方法。FedAvg 通過將各客戶端 (Client) 本地訓練的模型權重進行加權平均來更新全局模型，有效減少了通信開銷並提升模型的整體性能。其演算法的核心步驟如下：

1. 伺服器初始化一個全局模型，並將其分發至參與訓練的邊緣設備。
2. 每個邊緣設備使用其本地數據在接收到的全局模型基礎

上進行數輪本地訓練，並計算更新後的模型權重。

3. 邊緣設備將更新後的模型權重傳回伺服器，伺服器根據每個邊緣設備的數據量對其模型權重進行加權平均。

4. 伺服器根據聚合後的權重更新全局模型，並重複上述過程直至收斂。

FedAvg 的應用不僅能充分挖掘每個區域的本地數據特性，還能通過多地區間的信息共享，提高模型對未知或跨區域崩塌事件的預測精度。此外，這種框架避免了將敏感地理及災害數據直接集中至單一伺服器，針對較廣泛的情況給予中央模型學習不同情況的能力。

第二節 工作執行步驟

一、資料整理

資料集製作方式：

為了針對崩塌發生區域較為密集的地區進行建模，本計畫採用聯邦學習方法，以各區域的客戶端模型資料訓練中央模型。此過程中的特徵資料處理步驟將作為後續資料集建置的標準，具體流程如下：

遮罩創建：使用 ArcGIS Pro 軟體為各客戶端區域生成遮罩，以準確篩選資料範圍。

網格切分：將遮罩區域切分為 20m x 20m 的網格單位，便於後

續的資料處理與分析。

資料擷取與建置：根據不同的分析目的，運用 ArcGIS Pro 中的「按遮罩擷取」功能進行資料網格化建置。

下圖標示了選定的客戶端區域。

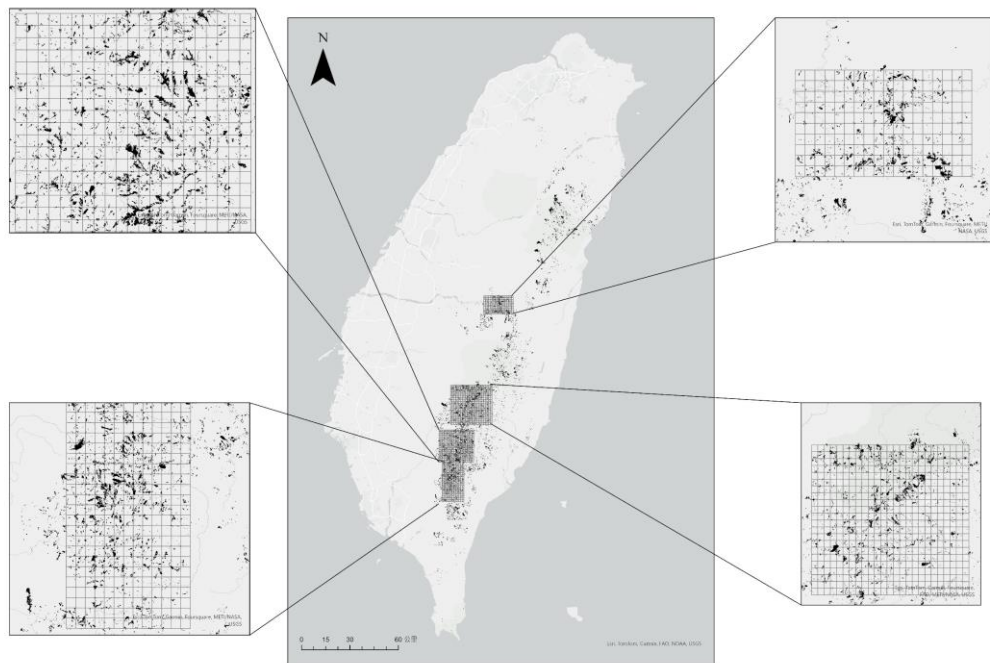


圖 6 、研究區域客戶端網格圖

由於崩塌發生區域主要集中於山區，本計畫選擇了中央山脈的三個崩塌事件密度較高的地點，建立了三組不同的資料集，作為客戶端模型的輸入來源。

(一)、崩塌資料

由於崩塌資料圖層原本為圖徵檔案，無法直接作為模型的輸入，

故先將其轉換為 20m x 20m 網格的點陣圖檔，圖中黑色區域表示崩塌區域，作為模型判斷是否發生崩塌的目標數據。

為了讓模型能夠辨識區域是否發生崩塌，需設定兩種類別標籤：崩塌（標籤為 1）與非崩塌（標籤為 0）。因此，除了崩塌區域外，也納入了非崩塌區域的數據供模型學習。最終，建置的資料集中在三個客戶端的崩塌與非崩塌比例均約為 2：8。

（二）、坡度及坡向

內政部所取得之數值高程地圖，藉由 ArcGIS Pro 內表面參數工具將其轉換為坡度與坡向資料。原始數值高程地圖即為 20m*20m 之點陣資料，因此無須額外進行轉換，將數值高程點陣圖輸入表面參數工具內，參數類型選擇 ”slope (坡度)” 、 ”aspect (坡向)” ，並利用先前所建置之客戶端區域遮罩進行截取轉換，即可取得目標區域地形之坡度、坡向點陣圖檔，結果如下圖 8 坡度圖、圖 9 坡向圖所示，中間為全台不分幅之數值高程圖、右上為測試區域、右下為客戶端 1、左上為客戶端 2 及左下為客戶端 3。

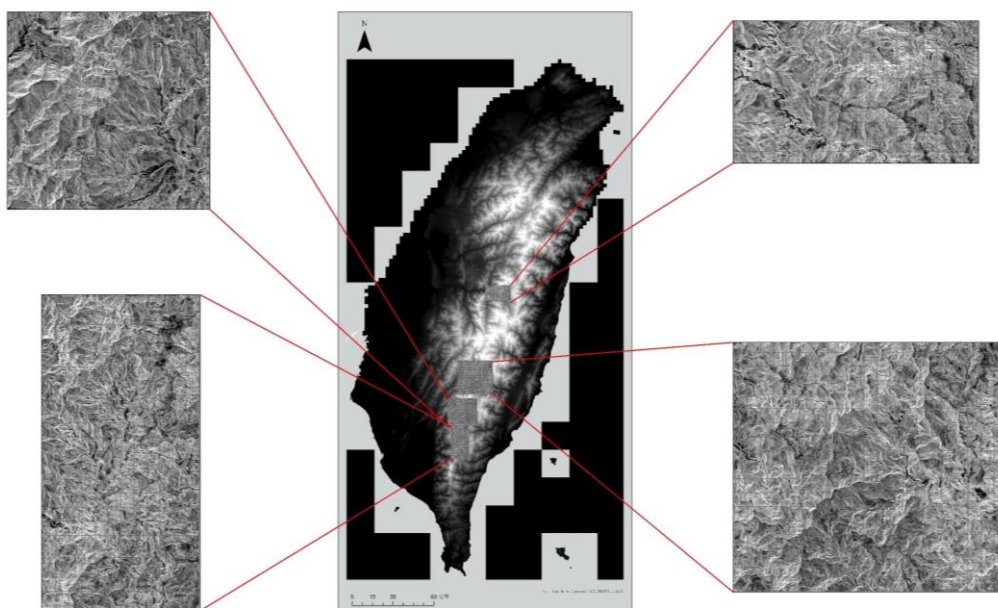


圖 7、客戶端目標區域坡度圖

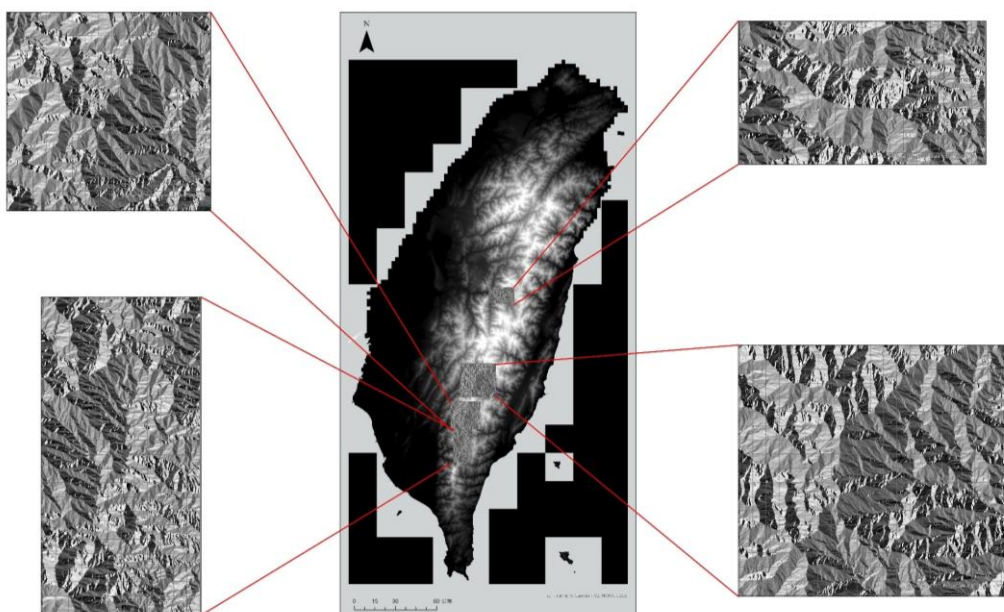


圖 8、客戶端目標區域坡向圖

(三)、雨量測站

從臺灣氣候變遷推估資訊與調適知識平台（TCCIP）取得的每日觀測資料，因其降尺度後的資料分佈為點資料格式，因此將

每個點位進行編碼，以確保每個網格單位的雨量點位數據來自距離最近的點位。具體操作步驟如下：

1. 首先將點資料轉換為點陣格式。此點陣的大小為降尺度後的網格尺寸(1km x 1km)，與最終目標網格尺寸(20m x 20m)不一致，後續本計畫區分兩種不同情況進行分析。
2. 將該點陣轉換為圖徵，避免受到原始網格大小邊界的限制。
3. 最後，將圖徵重新轉換為 20m x 20m 的點陣格式，並利用先前建立的目標區域遮罩進行截取，確保每個網格單位的雨量值取自距離最近的 TCCIP 網格點資料。

下圖為網格雨量點位資料取得圖。

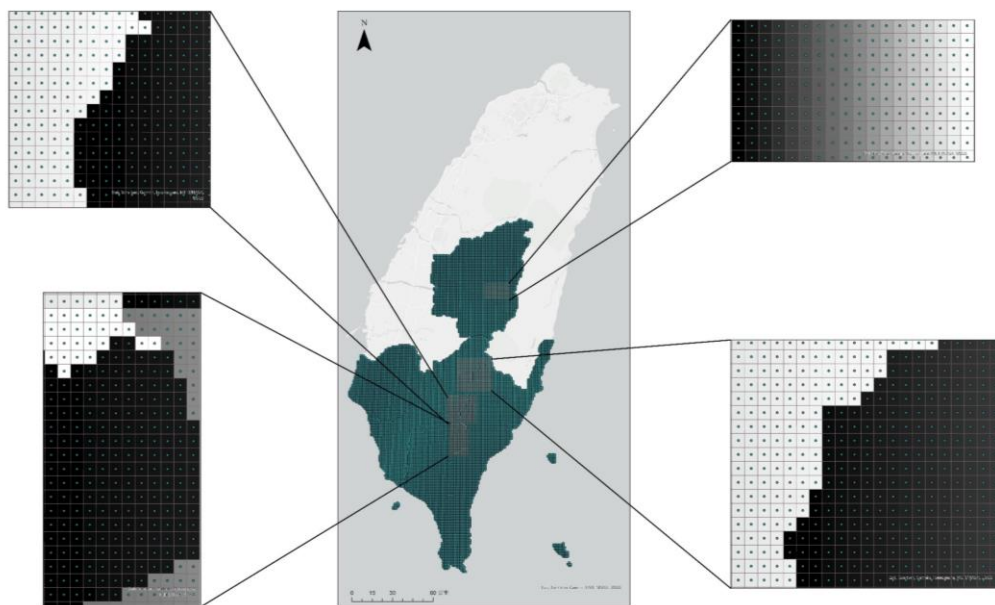


圖 9、客戶端目標區域雨量點位圖

(四)、資料整理結果疊合與切割

為了建立有效的模型訓練資料集，本計畫將上述整理的結果，包括 20m x 20m 網格之崩塌標籤、坡度、坡向，以及兩種不同解析度（1km x 1km 與 20m x 20m）的雨量點位編碼，輸出為 TIFF 檔案並進行疊合。最終得到三個客戶端資料集，其筆數分別為 12,360 筆、7,875 筆及 18,252 筆，中央模型測試資料集則為 18,460 筆。詳情見下表。

每筆資料包含 4 個通道，分別代表坡度、坡向、雨量點位編碼及崩塌標籤。雨量點位編碼與整理好的雨量表鏈結，從而獲得對應的雨量數據。本計畫設定的模型輸入雨量為 2 日累積雨量。

表 1、各客戶端與測試區資料表

	Client1	Client2	Client3	TestData
資料筆數	12360	7875	18252	18460
資料形狀	(12360, 4)	(7875, 4)	(18252, 4)	(18460, 4)

(五)、資料正規化

在模型構建過程中，資料正規化是一個關鍵步驟，旨在使不同範疇的輸入特徵具有相似的數值範圍，以促進模型訓練的穩定

性和效率。以下是針對本計畫資料正規化的具體說明：

崩塌標籤為二元分類資料，以 1 表示崩塌區域，0 表示非崩塌區域。由於該資料的取值範圍已在 0 到 1 之間，因此不需要額外正規化，但可進一步確保標籤格式的一致性，方便後續模型訓練。

坡度 (Slope) 通常會取值於一定範圍，隨地形不同而變化。為了將坡度數值縮放至 0 到 1 之間，本計畫採用最大最小正規化 (Min-Max Normalization)，計算公式如下：

$$S_{norm} = \frac{S - S_{min}}{S_{max} - S_{min}}$$

其中 S 為原始坡度值， S_{min} 和 S_{max} 分別為坡度的最小值和最大值。這樣的轉換能標準化坡度數據，並有助於模型學習。

坡向 (Aspect) 通常用角度表示，範圍在 0 至 360 度之間。為了標準化該特徵，可以將角度除以 360，將其範圍縮放至 0 到 1 之間，計算公式如下：

$$A_{norm} = \frac{A}{360}$$

此方法保留了角度信息，避免了大範圍數值對模型訓練的影響。

本計畫將雨量數據正規化為 2 日累積雨量。由於不同區域和降雨事件的雨量範圍可能差異較大，在此採用 Z-score 正規化 (Z-

Score Normalization)，計算公式如下：

$$R_{norm} = \frac{R - \mu_R}{\sigma_R}$$

其中 R 為累積雨量， μ_R 為所有樣本的平均累積雨量， σ_R 為其標準差。這樣的標準化能幫助模型在不同氣候區域中識別異常降雨情況，提高模型對異常事件的敏感性。

完成正規化的資料集有效減少數值範圍的差異，使模型更專注於不同特徵間的相對影響，從而提高訓練速度和模型的預測性能。這一系列的正規化過程為模型的訓練奠定了堅實的基礎，旨在提升對崩塌事件預測的準確性和穩定性。

二、模型建構

(一)、模型架設

此模型使用 PyTorch 深度學習框架，以自定義類別 SimpleNet 架設基本神經網路架構，通過堆疊各種全連接層及活化函數來構建深度學習模型。模型架構的層數、節點數量及活化函數皆已依據本計畫需求設置，具體配置如下：

第一層：全連接層 (fc1)，包含 128 個節點，輸入 3 個特徵，並使用 ReLU 活化函數進行非線性轉換。

第二層：全連接層 (fc2)，包含 64 個節點，接續上一層輸出，

並使用 ReLU 活化函數。

第三層：全連接層 (fc3)，包含 32 個節點，並使用 ReLU 活化函數。

第四層：全連接層 (fc4)，包含 16 個節點，使用 Sigmoid 活化函數，使輸出值範圍介於 0 到 1 之間。

輸出層：全連接層 (fc5)，包含 2 個輸出節點，對應於二元分類的兩個類別。

在模型的正向傳遞過程中，輸入數據經過每層的全連接層及活化函數處理，最終輸出二元分類的預測結果。本架構設計適合二元分類任務，並藉由逐層轉換，實現對輸入數據特徵的有效學習。

(二)、優化器及學習率設定

深度學習模型中的優化器是訓練過程的關鍵組成部分，旨在透過調整模型權重以最小化損失函數，從而提升模型性能。常見的優化器包括隨機梯度下降 (Stochastic Gradient Descent, SGD)、RMSprop (Root Mean Square Propagation) 及 Adam (Adaptive Moment Estimation) 等。

本計畫中所使用的優化器為隨機梯度下降 (SGD)，該優化器透過對每個客戶端模型的權重進行逐步更新，以加速損失函數的收斂。SGD 以其隨機性和簡單的更新方式著稱，能在一定程度上避免陷入局部最小值。在每次更新中，學習率 (learning rate) 設定為 0.01，控制每次權重調整的幅度。

學習率作為一個重要的超參數，決定了模型更新權重的步伐大小。選擇合適的學習率對於模型的收斂速度和性能有著至關重要的影響：過大的學習率會導致在目標函數的最小值附近震盪，甚至可能導致發散，而過小的學習率則會使模型收斂速度減慢，增加訓練時間，並可能陷入局部最小值。

SGD 優化器在每次訓練迭代中保持固定學習率，儘管這種設置簡單直接，但需要謹慎調整以適應模型的不同訓練階段。本研究採用了固定學習率 0.01，旨在確保穩定的收斂速度。

(三)、損失函數設定

損失函數 (Loss Function) 是在機器學習和統計模型中量化預測值與真實值之間差異的重要工具。常見的分類問題損失函數包括交叉熵損失 (Cross-Entropy Loss)、二元交叉熵 (Binary Cross-Entropy) 及 Hinge 損失等。本計畫針對崩塌事件的預測任務，選用了自定義

的被最大熵法 (BME Entropy Loss) 損失函數，以改進模型在訓練過程中的穩定性和泛化性能。

BME Entropy Loss 損失函數結合了傳統交叉熵損失與熵正則化項，設計理念為在標準交叉熵損失的基礎上引入熵調整，使模型學習過程中具有更多的不確定性考量，從而更具韌性。具體構造如下：

交叉熵損失：BME Entropy Loss 中的主要成分為交叉熵損失，用於衡量模型預測的類別分佈與實際標籤之間的差異。交叉熵能夠有效地處理多分類問題，並促使模型生成準確的分類概率。

熵正則化項：通過引入預測分佈的熵項，該損失函數在不確定性較高的情況下對模型進行正則化處理。熵的計算方式為對每一類的預測概率取對數，並與概率本身相乘以獲得平均值。最終損失公式包含了熵正則化項，並以參數 α 控制其強度。

最終損失計算公式為：損失 = 交叉熵損失 - α * 熵，其中 α 控制正則化項的影響力。這一結合設計能有效促進模型在不同特徵分佈下的適應性，提高模型泛化能力。

(四)、聯邦學習訓練步驟

在本研究中執行聯邦學習的訓練流程，旨在有效地整合各個客戶端的模型權重，並通過迭代的方式提升中央模型的性能。訓練過程分為多個回合，每一回合都包含一系列步驟，以確保中央模型和客戶端模型的持續優化。以下是具體的訓練步驟描述：

客戶端模型訓練：針對不同的客戶端區域，將前述步驟所整理好的資料入模型以進行訓練，訓練完成後取得所有模型內的參數。

聚合權重至中央模型：從各個客戶端提取出的權重，進行加權聚合，將聚合後的權重加載到中央模型中。

評估中央模型：聚合後的中央模型會進行評估，計算 F1-score 以衡量模型在驗證數據上的性能。此步驟不僅有助於了解當前模型的表現，還為後續訓練過程提供了最佳化的方向。

紀錄與繪製混淆矩陣：在每一回合結束時，會紀錄當前回合的混淆矩陣資料，以便分析模型的預測結果。透過對比真實標籤與預測標籤，混淆矩陣能直觀地展示模型在不同類別上的預測準確性。

更新客戶端模型權重：若中央模型的 F1-score 優於之前最佳的準確度，則更新最佳準確度的記錄，並重置未改善的回合計數；否則，

未改善的回合計數將增加。如果達到預設的最大回合次數，則終止訓練過程，避免過度擬合。

重新訓練客戶端模型：所有客戶端模型將使用中央模型的權重進行更新。透過訓練客戶端模型，確保每個客戶端在其本地數據上持續學習，以增強模型的泛化能力。

這樣的訓練流程使得模型能夠在不直接訪問客戶端數據的情況下進行有效學習，並充分利用各個客戶端的計算能力，最終使模型有更好的預測性能。此研究的聯邦學習方法不僅提高了數據隱私的保護，也促進了模型在多樣化數據上的適應性。圖 10 為本次研究模型學習架構圖。

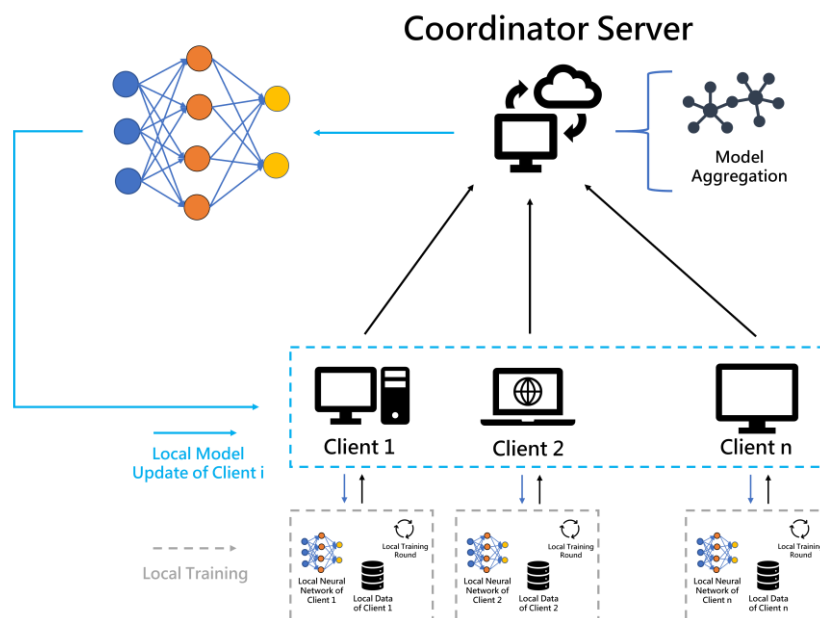


圖 10、聯邦學習架構圖

(五)、模型任務

由於降雨數據解析度與崩塌資料解析度之間的差異，本計畫設計了兩種不同的模型預測目標，以評估聯邦學習是否能夠顯著改善模型的預測能力。

目標一：回歸任務

第一個工作目標旨在預測 1 公里網格內的崩塌面積比例；為了實現這一目標，本研究將相關的地形特徵重新取樣至 1 公里的解析度，與雨量網格大小一致，確保所有資料的解析度統一，並且統計原本 1 公里網格內，解析度為 20 公尺的崩塌網格。透過此方法，模型將能夠提供每個 1 公里網格中崩塌區域的比例預測，這對於深入理解地區性崩塌風險及其潛在影響範圍至關重要。

目標二：分類任務

第二個情況主要在於判斷每個 20 米解析度的網格單元是否為崩塌區域。該模型將使用轉換後的 20 米解析度雨量資料作為輸入，以預測崩塌事件的發生。這一方法旨在提高對於局部崩塌風險的識別能力，從而為災害管理提供更精確的依據。

這兩個不同目標的分析將為提供更深入的觀察，幫助評估聯邦學習在提升預測準確性方面的效果。

(六)、評估指標

評估指標 (Evaluation Metrics) 是用來衡量機器學習模型性能的重要工具，不同的指標適用於不同的目標。在分類問題中，常見的評估指標包括混淆矩陣 (Confusion Matrix)、準確率 (Accuracy)、F1-score，以及 ROC-AUC 曲線 (Receiver Operating Characteristic - Area Under Curve)。選擇合適的評估指標對於準確評估模型性能和指導模型改進至關重要。

由於本計畫的目標是預測是否發生崩塌的分類任務，因此本計畫選用準確率作為初步的評估指標。準確率定義為正確預測的數量與總預測數的比值，雖然其簡單易懂，但在類別不平衡的情況下，僅依賴準確率可能無法正確反映模型的表現。為了獲得更全面的評估，同時使用混淆矩陣來計算其他重要指標，如精確率 (Precision)、召回率 (Recall) 及 F1-score，這些指標能提供模型在不同方面的表現評估。

此外，ROC-AUC 曲線作為另一個重要的評估指標，可以有效衡量模型的分類能力。ROC 曲線描繪了真正率 (True Positive Rate) 與假正率 (False Positive Rate) 之間的關係，而 AUC 值則表示模型區分

正類和負類的能力。這些評估指標共同構成了一個全面的性能評估體系，幫助此研究更深入地理解模型在崩塌預測任務中的表現，說明如表 2。

表 2、混淆矩陣表

混淆矩陣	預測無崩塌 (yp = 0)	預測有崩塌 (yp = 1)
真實無崩塌 (yt = 0)	真陰性 (TN)	假陽性 (FP)
真實有崩塌 (yt = 1)	假陰性 (FN)	真陽性 (TP)

■精確率(Precision)：
$$\frac{\text{真陽性}(TP)}{\text{真陽性}(TP) + \text{假陽性}(FP)}$$

■召回率(Recall)：
$$\frac{\text{真陽性}(TP)}{\text{真陽性}(TP) + \text{假陰性}(FN)}$$

■F1-Score：
$$2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$$

此三者的特點為精確率度量在所有預測為正的樣本中，實際為正的比例，適合於錯誤正類（假陽性）代價高的情況；召回率度量在所有實際為正的樣本中，被正確預測為正的比例，適合於錯誤負類（假陰性）代價高的情況；F1 分數則綜合考慮精確率和召回率的調和平均數，適合於精確率和召回率都很重要的情況。

第三章 工作進度與交付項目

第一節 計畫甘特圖

工作項目	年別	113年											
	月份	2	3	4	5	6	7	8	9	10	11	12	
資料蒐集													
資料整理													
建置當地模型													
建置聯邦學習架構													
模型訓練與調整													
表現評估													
期中報告撰寫													
期末報告撰寫													

圖 11、本計畫甘特圖

計畫時程如下

2～4 月：

- 蒐集崩塌相關資料
- 蒐集雨量相關資料
- 異質資料彙整、統合
- 相關文獻蒐集

5～7 月：

- 當地模型建置
- 當地模型效果評估

8～11 月：

- 聯邦學習架構設置

■模型整體效果評估

11 ~ 12 月：

■模型結果整合

■模擬結果上傳

■文章/期刊撰寫

第二節 計畫交付項目

整合不同來源資料

目前輸入模型所使用之資料為 tiff 檔案，裡面包含 3 種不同特徵，分別為坡度、坡向及崩塌當日之前 2 日累積雨量，整理方式為應用 ArcGIS Pro 內圖徵-點陣轉換、點-圖徵-點陣轉換等方式將資料轉換成可以使用及編輯的形式，亦包含降尺度網格點建置編號並匹配至目標網格之做法，利用 python 語法將整理好之雨量點位編號對應至儲存著日雨量的表格內，並將上述不同來源之資料整理完後堆疊與切割成不同情況所需應用之資料格式，其可以匯入的資料即可包含圖徵、圖磚、單一點位測站及降尺度多網格點。

模型目前結果

回歸目標結果：

圖 12 為聯邦學習系統在前 5 回合中的模型預測結果，包括中央模型和各客戶端模型的表現。散點圖中，橫軸為真實值，縱軸為模型的預測值，紅色虛線則代表理想預測線 (True Values = Predicted Values)，即當預測值完全正確時的參考線。在這個早期階段，可以觀察到大多數預測值集中於低區間並分散於紅色虛線下方，說明模型在初始幾回合中尚未能有效捕捉數據的分佈特徵，且對目標變量的預測能力有限。這種偏低的預測表現可能是因為模型還處於學習初期，參數尚未充分更新，也可能是因為各客戶端的數據分佈異質性導致模型難以在短期內達成一致。

此外，不同客戶端模型的表現並不一致，這可以反映出聯邦學習環境下，各個客戶端由於數據特性不同而對模型訓練的貢獻有所差異。這種差異會隨著訓練回合的增加逐漸被中央聚合模型所調整，但在早期回合中依然較為顯著。

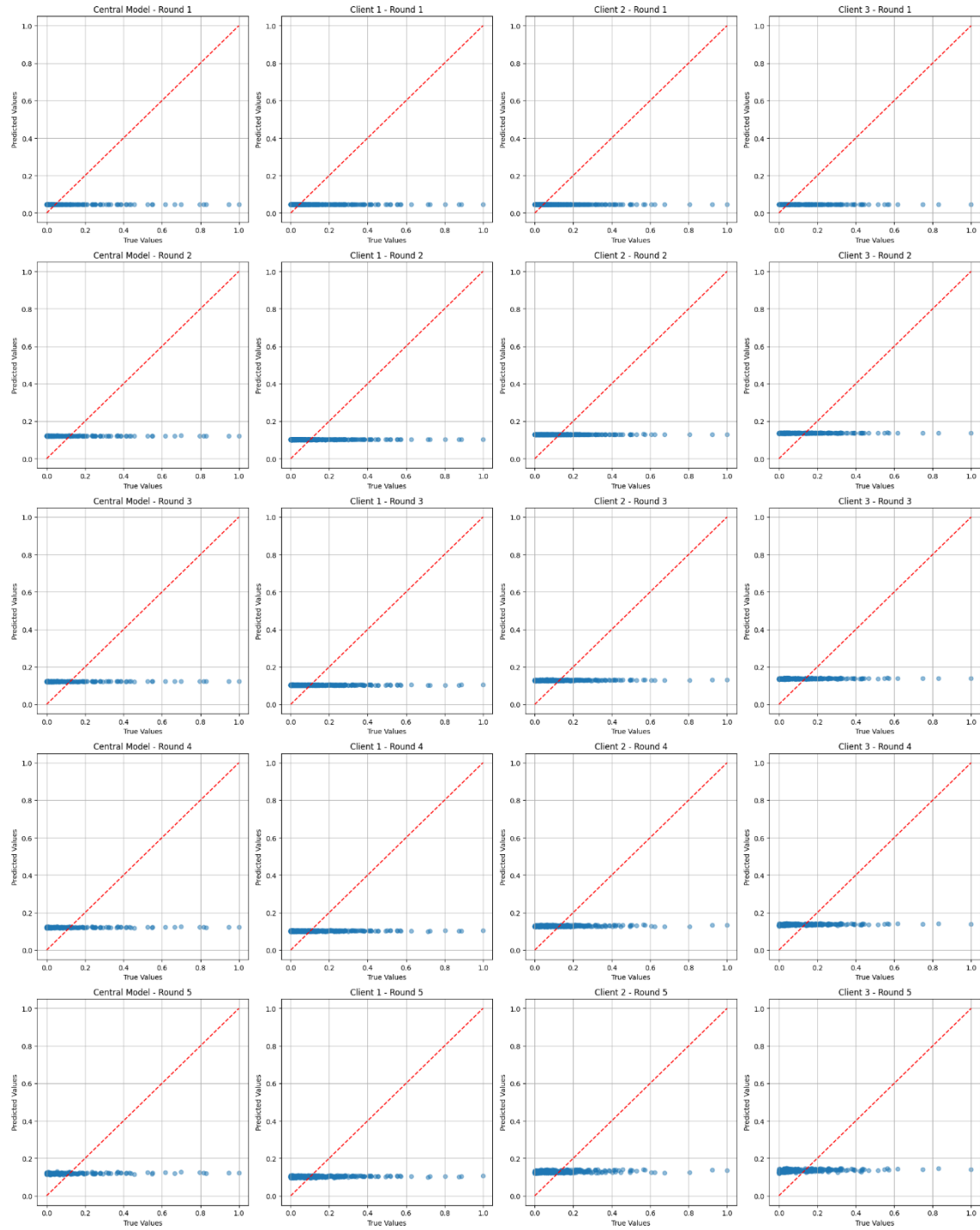


圖 12、聯邦學習 1~5 回合迴歸結果圖

圖 13 展示了聯邦學習系統在第 6 到第 10 回合的模型預測結果，顯示出相比前 5 回合，模型的學習效果有所改善。隨著回合數的增長，模型參數通過更多次的聯邦聚合逐漸調整，預測值與真實值之間的偏差減少，可以看到更多的散點向紅色虛線靠近。這說明隨著每回合的模型更新，中央模型逐漸獲得了各客戶端數據的全貌，進一步提升了對數據模式的學習效果。此時，預測結果雖然依然集中於較低區間，但點的分布趨勢已逐漸向理想預測線趨近。

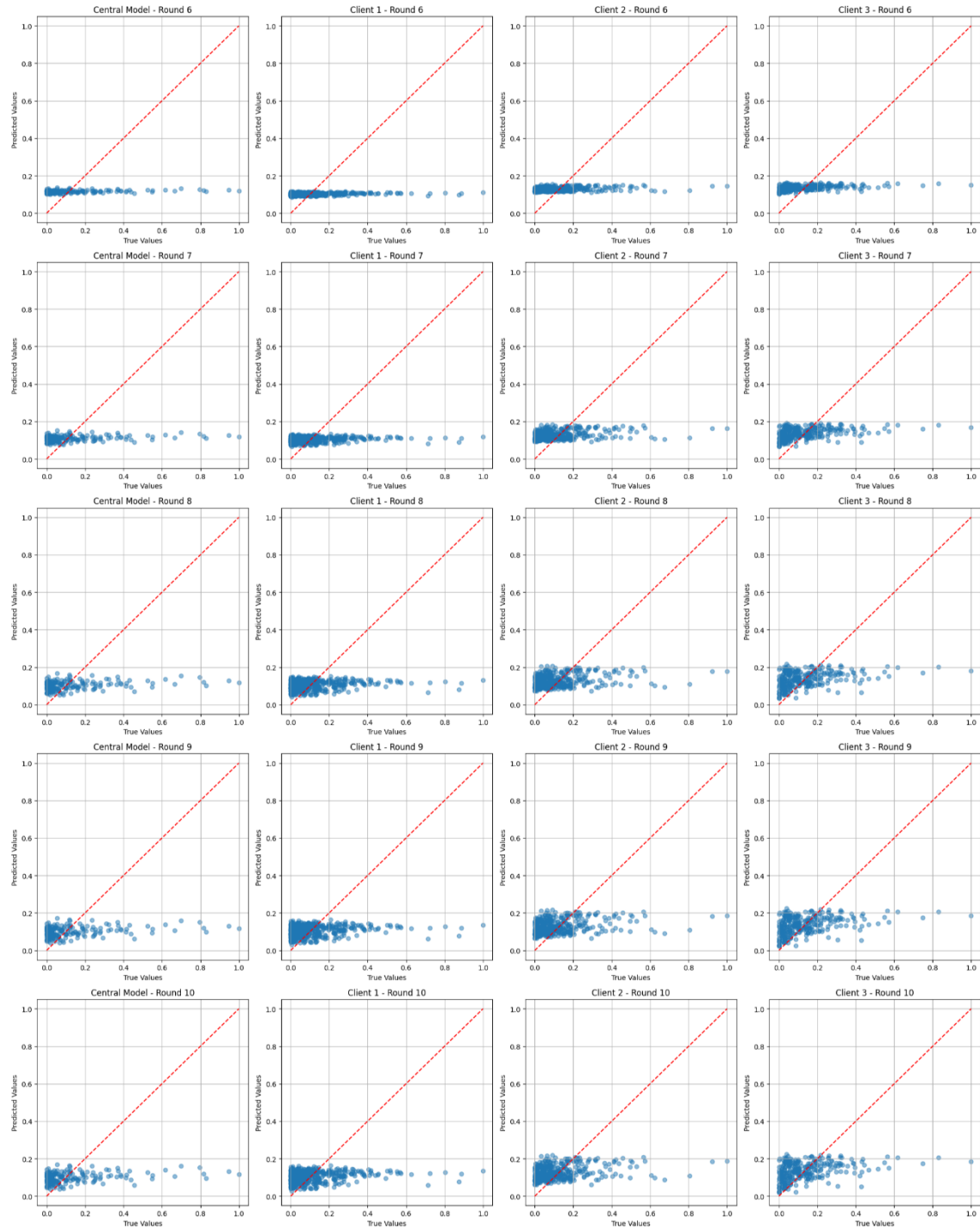


圖 13、聯邦學習 6~10 回合迴歸結果圖

在圖 14 中，展示的是模型經過 61 到 65 回合訓練後的預測結果，即模型學習的最終成果。可以看到，相比前面的回合，預測值更加接近紅色虛線，顯示模型在聯邦學習過程中已達到較穩定的狀態。散點分佈更加均勻，且大量點數靠近理想預測線，說明模型的預測準確度顯著提高，能夠更準確地擬合數據分佈。

在聯邦學習的後期階段，中央模型通過多次的更新和聚合，成功融合了來自各客戶端的數據信息，使得模型參數穩定收斂，最終達到較佳的預測效果。此外，各客戶端模型的表現也趨於一致，顯示出聯邦學習的協同效應充分發揮，讓不同數據特性的客戶端在聯合學習下達到協同進步。這種收斂效果說明聯邦學習的長期穩定性，即在聯邦學習環境中，即便在數據分佈異質性較大的情況下，仍能通過多輪次聚合達到良好的模型性能。

在這個階段，各客戶端模型的表現仍存在些微差異，不過隨著聯邦學習過程的進行，各模型在中央聚合的影響下逐漸向一致性收斂。這表明聯邦學習機制在此回合數範圍內正逐步發揮其協同學習效果，使得整體模型性能得以穩步提升。

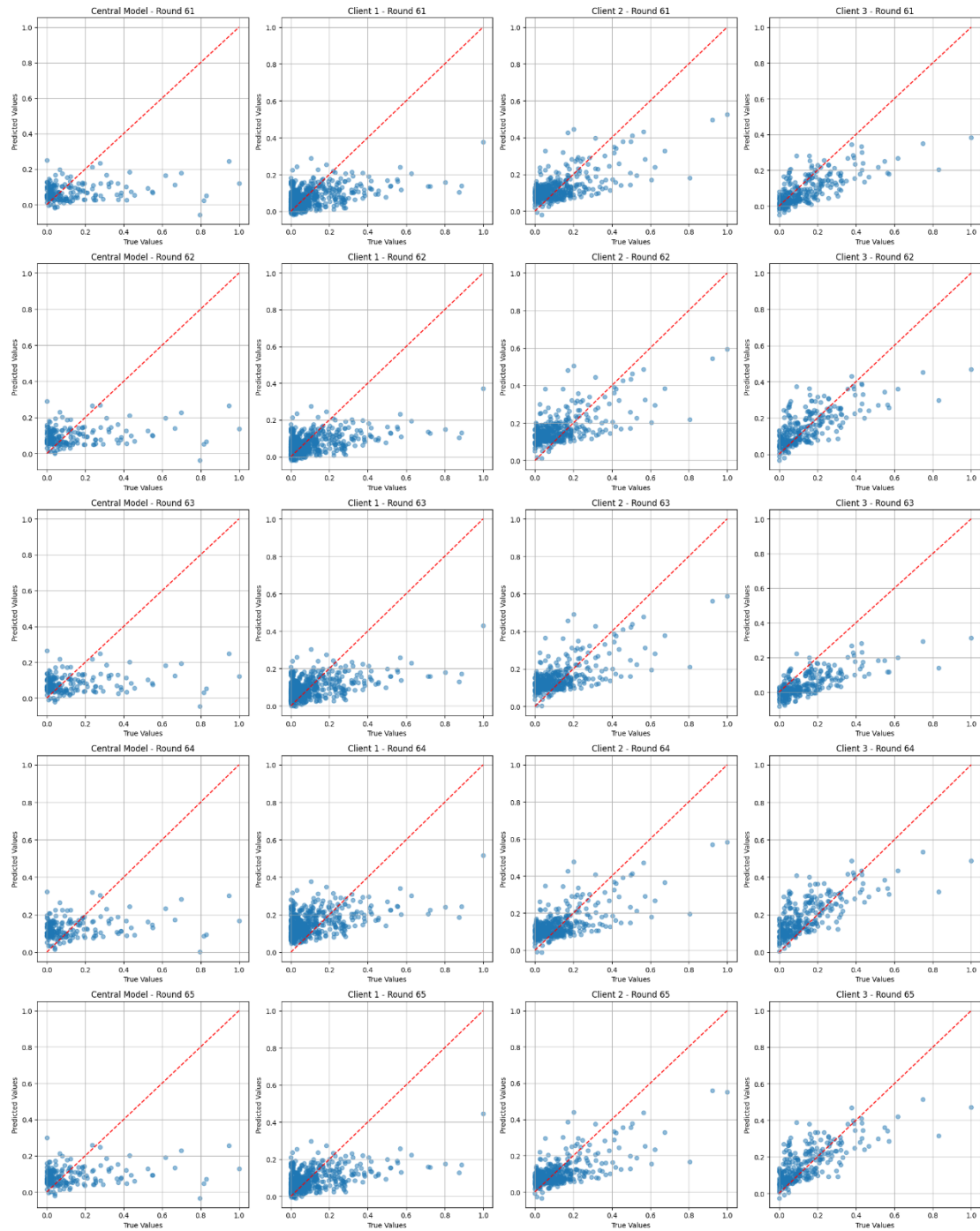


圖 14、聯邦學習 61~65 回合迴歸結果圖

分類目標結果：

圖 15 為聯邦學習模型在前 5 回合的表現。從這幾個回合的混淆矩陣中可以明顯看到，中央模型和每個客戶端模型在崩塌事件的識別上表現非常有限。在這個階段，模型主要預測的結果偏向於標記為 0 的非崩塌事件，幾乎無法辨識標記為 1 的崩塌事件。具體而言，中央模型和客戶端模型的預測結果顯示了極高的負樣本識別率，但對於正樣本（崩塌事件）的捕捉卻非常缺乏。這個現象表明，在訓練初期，模型對於崩塌事件的特徵學習不足，尚未能有效區分崩塌與非崩塌事件。由於崩塌事件的樣本數較少，模型在早期可能更傾向於預測為大多數類別（即非崩塌事件），導致偏誤。這樣的初始結果也反映出聯邦學習中各客戶端模型在未經多回合同步的情況下，難以單獨學習到少數類別的特徵。



圖 15、聯邦學習 1~5 回合分類結果圖

圖 16 展示了模型在第 6 至第 10 回合的表現，可以發現此階段的模型在識別崩塌事件方面開始有所改善。隨著回合的增加，各客戶端模型不斷進行權重更新並與中央模型進行同步，逐步地提高了對崩塌事件的辨識能力。具體來說，從第 8 回合開始，中央模型和部分客戶端模型逐漸能夠識別出一些崩塌事件（標記為 1 的情況）。混淆矩陣中出現了少量的正樣本預測，代表模型在這一階段開始學到了一些有助於辨識崩塌事件的特徵。這反映出聯邦學習架構下的權重聚合機制，使得各客戶端模型能在相對有限的資料下逐漸學習到整體資料集的特徵，並提升崩塌事件的辨識準確度。雖然在這一階段的混淆矩陣中，模型對崩塌事件的預測仍然有限，但顯示出模型正在逐漸突破初期的偏誤，並開始建立更平衡的預測能力。



圖 16、聯邦學習 6~10 回合分類結果圖

圖 17 為聯邦學習模型以分類為目標的最終成果（第 47 至第 52 回合）的混淆矩陣。經過多次回合的訓練和權重更新後，模型已經能夠相對準確地識別崩塌事件。無論是中央模型還是各個客戶端模型，對於崩塌事件的辨識準確度都有顯著提升，並且模型的預測結果在正、負樣本之間達到了一定的平衡。最終回合的混淆矩陣顯示出，模型在崩塌事件的辨識上已經不再受到初期偏向非崩塌事件的影響，而是能夠有效捕捉到崩塌事件的發生。這樣的結果顯示聯邦學習在多回合訓練過程中對模型性能的提升效果，特別是在少數類別的辨識上，中央模型透過每輪權重聚合，有效地結合了各個客戶端模型的學習成果，從而提升了整體的分類表現。最終的成果反映出模型在聯邦學習架構下，經過多次回合的協同學習後，具備較穩定的模型表現。



圖 17、聯邦學習 47~52 回合分類結果圖

從圖 18 中的 ROC-AUC 結果可以觀察到，模型在崩塌事件預測中的 AUC 值為 0.66。AUC (Area Under the Curve) 值為 0.66 表示模型在不同閾值下能夠適度地區分崩塌與非崩塌區域，然而模型的預測能力仍在中等範圍內，未達到高度精確的水準。具體而言，AUC 值為 0.66 意味著模型的預測效果僅略高於隨機猜測 (AUC = 0.5)，顯示模型具備一定的識別崩塌區域的能力，但尚不足以應用於高精度需求的實務場景。

該結果反映了模型在訓練數據中捕捉到了一些重要的特徵模式，能夠在一定程度上區分崩塌與非崩塌情況。然而，這樣的結果也指出模型可能尚未完全學習到崩塌事件的關鍵影響因素，或者訓練數據特徵在解釋崩塌事件上存在一定的侷限性。

未來優化的方向可以包括進一步提升模型結構與參數的調整，增加訓練資料集中特徵的多樣性，或引入更多高相關性的地理或環境特徵數據，以改善模型的表現。此外，考慮聯邦學習在分散式資料上的應用，逐步提升模型在各個客戶端的學習效果，可能能夠更有效地提高模型在崩塌事件預測上的準確性。這樣的改進預計會在未來的研究中，逐漸提升模型的 AUC 值與預測能力。

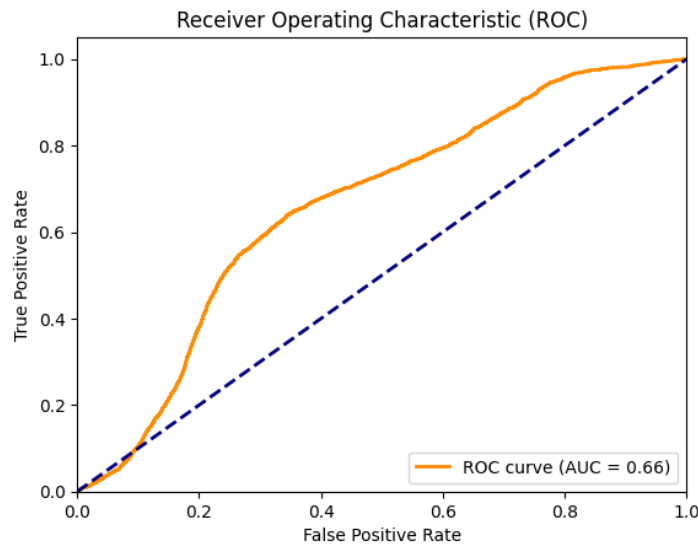


圖 18、ROC 及 AUC 結果圖

透過上述兩種不同任務的觀察可以發現，網格單元大小的差異對模型表現具有顯著影響，經由回歸任務與分類任務的比較得知，採用相同網格單元大小進行研究能夠提供更高的結果可靠性與實用性，因此本計畫重新採用卷積神經網路 (CNN) 對回歸任務進行模擬與訓練，並獲得以下結果。

圖 19 顯示了 CNN 融合聯邦學習架構後進行整體訓練的前五回合結果。從圖中可以看出，自第二聯邦學習回合開始，模型性能便顯著提升，隨著訓練回合數增加，CNN 模型的表現相比 ANN 模型有顯著改善。圖 20 展示了同一訓練回合下 ANN 模型與 CNN 模型的回歸結果對比（上圖為 ANN 模型結果，下圖為 CNN 模型結果）。CNN 模型的相關回歸統計指標詳列於表 3。

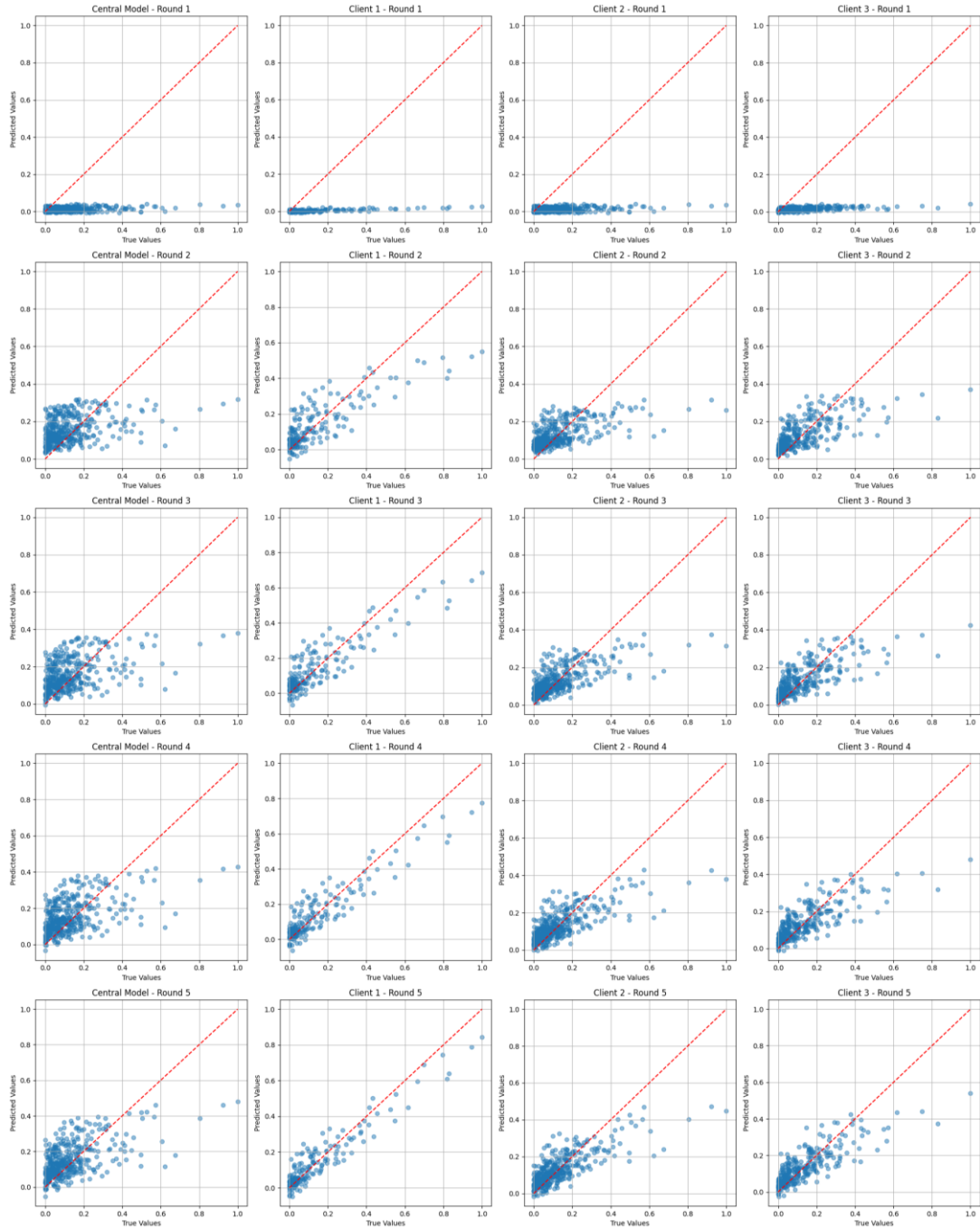


圖 19、聯邦學習 1~5 回合 CNN 迴歸結果圖

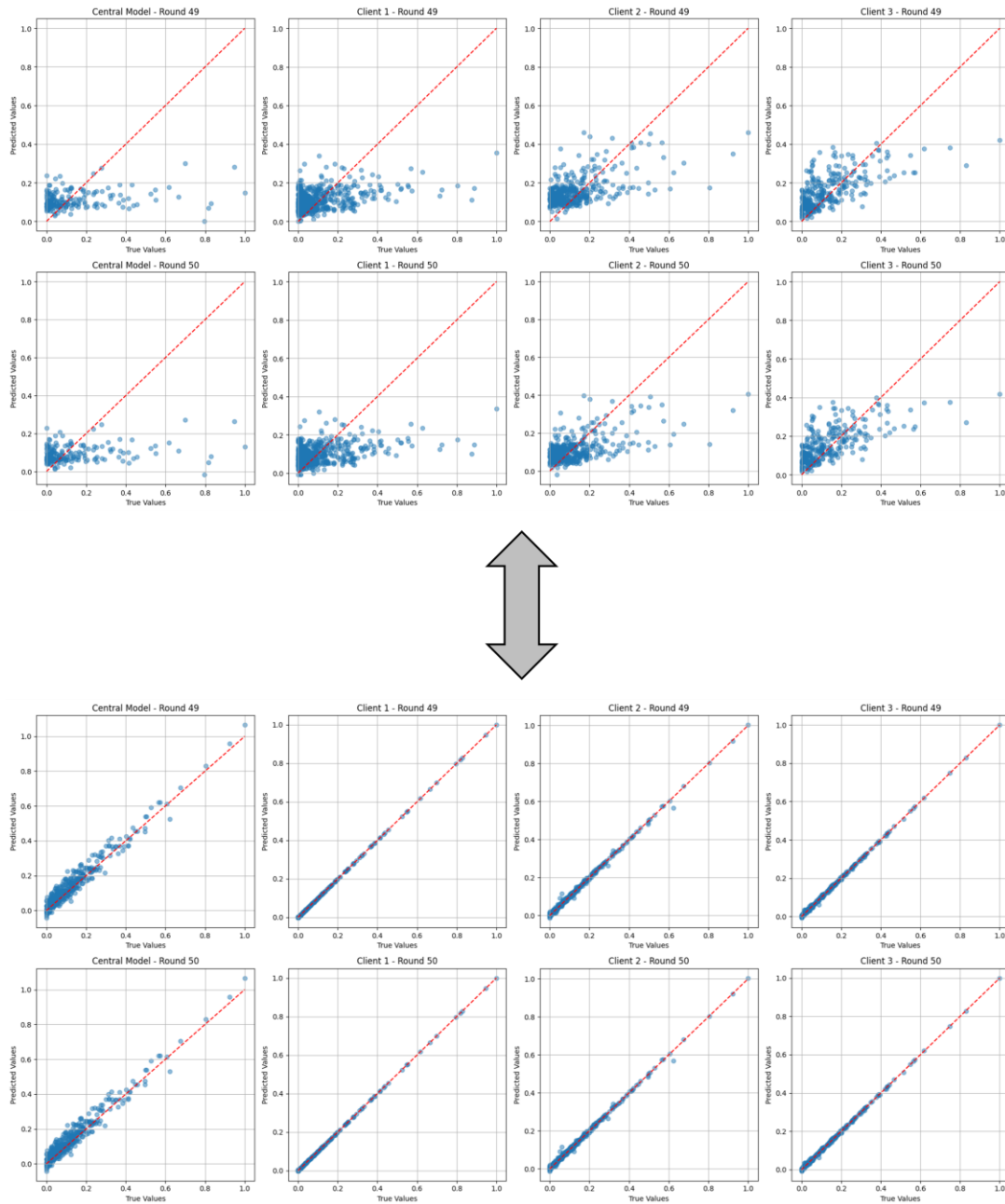


圖 20、ANN、CNN 模型 49~50 回合結果比較圖

表 3、CNN 回歸結果統計指標表

	RMSE	Bias	ubRMSE	NSE	Correlation
Center Server	0.06	-0.04	0.04	0.89	0.98
Client 1	0.01	0.01	0.01	0.99	0.99
Client 2	0.09	-0.06	0.08	0.73	0.94
Client 3	0.09	-0.07	0.06	0.78	0.96

綜上所述，本研究透過聯邦學習框架逐步聚合和更新中央模型與各客戶端模型的權重，有效促進了模型從多方數據中學習到崩塌特徵的能力，在聯邦學習的架構下，模型能在不同數據來源之間實現協同學習，克服了數據分散的挑戰，此過程不僅顯著提升了模型的整體預測準確性，還通過充分利用各區域內特定的崩塌特徵，使模型具備更強的泛化能力與適應性，透過權重的動態更新，中央模型能逐步匯總各地區的數據特性，實現對崩塌現象的全面學習，同時該架構的協同學習特性不僅促進了數據共享的效率，也為後續多場景、多應用的擴展提供了良好的基礎，未來，透過引入更為精細的數據特徵工程與模型優化策略，聯邦學習框架有望在災害預測與風險管理領域發揮更大的作用。

第四章 結論及建議

第一節 結論

截至目前為止，已完成資料蒐集、資料整理、建置當地模型建置聯邦學習架構。

資料從不同地方取得，其網格大小、資料型態及內容均有所不同，利用 ArcGIS Pro 內之功能可以有效率且方便的進行統整，產生針對區域性的有效資料集，並透過 python 語法將資料整合、堆疊及切割，完成模型訓練資料集蒐集，結果如前表 1 所示。

目前當地模型之神經網路已完成建置，其架構即為前述之模型架構，含有 1 輸入層、1 輸出層與 3 層隱藏層，並分別設有不同個數的神經元數量，輸入的資料檔內堆疊坡度、坡向及 2 日累積雨量資料，目標的標籤資料為代表有發生崩塌的“1”與未發生崩塌的“0”。

本計畫確立了聯邦學習的架構，包括梯度計算、資訊交換及模型聚合。具體流程如下：首先在客戶端進行模型訓練，接著將權重提取至中央模型，隨後對中央模型進行測試。完成測試後，將中央模型的權重提取並重新分配給各客戶端模型，進行權重更新和重新訓練。透過這一系列步驟，成功實現了聯邦學習的架設與運作。

第二節 建議

本計畫已使用較為簡單的模型架構將聯邦學習的概念實作，其產生的結果與原本沒有使用聯邦學習架構而進行機器學習的結果還要好，後續開始嘗試使用更為複雜的模型對崩塌抓取進行更深入的使用。

參考文獻

1. 行政院農業委員會水土保持局，"水土保持應用手冊"，2005。
2. 中興工程顧問社，"降雨引發山崩預警資訊系統"，2018。
3. 李秉乾、雷祖強、謝孟勳、黃亦敏、方耀民、周天穎"應用人工智慧技術發展坡地崩塌風險 評估模式"，2019。
4. LeCun, Yann, et al. "Backpropagation applied to handwritten zip code recognition." Neural computation 1.4 (1989): 541-551.
5. Chen, Li, et al. "Beyond human recognition: A CNN-based framework for handwritten character recognition." 2015 3rd IAPR Asian Conference on Pattern Recognition (ACPR). IEEE, 2015.
6. Li, Li, et al. "A review of applications in federated learning." Computers & Industrial Engineering 149 (2020): 106854.
7. Rieke, Nicola, et al. "The future of digital health with federated learning." NPJ digital medicine 3.1 (2020): 1-7.
8. Nguyen, Dinh C., et al. "Federated learning for internet of things: A comprehensive survey." IEEE Communications Surveys & Tutorials 23.3 (2021): 1622-1658.
9. Park, Soohyun, et al. "Large-scale water quality prediction using federated sensing and learning: A case study with real-world sensing big-data." Sensors 21.4 (2021): 1462.

附錄

附錄一、期初審查會議紀錄暨回覆辦理情形

項次	審查意見	回覆辦理情形
報告內容審查意見：		
一、	為配合本署業務需求，計畫內容建議調整(或納入後續執行評估參考)部分：	
1.	所謂聯邦學習方法之應用案例為何？是否可有說明？其應用在崩塌災害預警有何案例可供參考？	感謝委員的提問，目前聯邦學習較常應用於醫學與金融方面；醫學類應用在於由於各醫院其病人病歷為保密資料，無法提供深度學習模型進行使用，導致在模型訓練上資料量相對不足也無法進行交叉比較，水平聯邦學習(horizontal federated learning)即可透過各醫院內部自己訓練之人工智慧模型，在不同樣本間擁有共同特徵的資料權重聚合到中央模型(Central)進行訓練，再將訓練結果更新回醫院端(Client)模型，提升模型預測能力。於金融方面，較常見的例

項次	審查意見	回覆辦理情形
		子為保險業可以透過蒐集不同消費者手機 apps 內部的演算法，及醫院中其病歷資料，產出之資料權重，在中央模型進行訓練，以此預測消費者偏好或是消費者習性，分析其可能生病機率，本種方法即為垂直聯邦學習(vertical federated learning)，為相同樣本不同之特徵值應用。 由於聯邦學習尚未廣泛應用於水文模擬預測，本計畫擬運用聯邦學習能夠接納資料不對齊及聚合不同模型權重之特性，將以往分開訓練個別建置之模型融合，在崩塌預警地的目標上，嘗試創造出兼容性更大，準確度更高之方法。
2.	本計畫將崩塌事件從數據資料將危險等級以資料科學之形式進行分類，提供辨識或劃分危險潛勢等級。採用統計方法，透過聯邦學習方法	感謝評審回復，本研究計畫基本可分以下之預期結果： (1)整理重要崩塌潛勢因子 (2)崩塌嚴重程度等級分類 (3)聯邦學習崩塌預警系統

項次	審查意見	回覆辦理情形
	建立多尺度之崩塌預警測，甚至進而準確預測崩塌之模型建立。由方法論觀之，採用各種模式之嘗試，不失為一電腦智慧之充分應用，惟其預期成果似未能具體說明，而無從掌握本研究可能之結果。	
3.	可能遭遇這困難：依賴於多個數據源，包括衛星影像、氣象數據和地面 監測數據。這些數據的質量、更新頻率和準確性直接影響崩塌地預測模型的可靠性。若數據質量不佳或更新不及時，可能會影響預測模型的效能。	謝謝委員的指導，目前了解到聯邦學習可以解決資料更新頻率不同的問題，不同的資料會在不同的客戶端(Client)進行訓練，輸入進中央模型的僅有權重，以此為特點處理一直以來在聚合不同類型資料時會產出之資料時間異質問題。數據質量及準確性會先透過統計方法，排除較不相關的資料，以盡可能減少資料噪音(data noise)為目標進行資料預處理，排除會影響預測模型效能之因子。

項次	審查意見	回覆辦理情形
4.	本案分析方法提及個別運算單元進行獨立運算並只對中央模型更新權重，其權重如何決定？	謝謝委員的提問，本研究計畫會以 Google 於 2016 年所發表之論文：Federated learning of deep networks using model averaging，所提出之 FedAVG 演算法進行聯邦學習訓練，其主要核心概念為權重整合 (Weight Aggregation)，主要執行方式為： (1) 權 重 收 集 (Weight Collection)：中央伺服器向參與訓練的設備發送請求，要求它們傳送其本地訓練模型的權重。 (2) 權 重 整 合 (Weight Aggregation)：中央伺服器收到來自各個設備的權重後，進行整合。這可以通過不同的方法來實現，例如簡單的平均，權重按參與設備的重要性進行加權平均，或者其他更複雜的整合方法。 (3) 中 央 模 型 更 新 (Global

項次	審查意見	回覆辦理情形
		Model Update)：整合後的權重被應用到中央模型中，並成為下一輪訓練的起點。
5.	福衛五號衛星目前取得之影像是否符合需求，請再斟酌。	感謝委員的建議，衛星資料在此模型屬於非必要的輸入，可以僅選取符合需求的部分進行輸入，目前已知福衛五號兩天更新一次資料，地面解析度為全色光- 2 公尺；藍光、綠光、紅光、近紅外光- 4 公尺。國家太空中心(TASA)所提供的示意圖可以藉由色塊分辨，但實際上是否使用模型進行分類需要經由實際的模型訓練來進行判斷，可能會遇到解析度不足等問題，也許可以使用其他的影像資料或實地調查的資料進行替代。

項次	審查意見	回覆辦理情形
6.	道路影像監視器畫面主要對象為路面，用作崩塌因子之輔助效果可再考慮。	感謝委員的建議，關於輸入資料的部分，道路影像監視器畫面為非必需的輸入因子，可以只擷取含有較多坡面的影像或者如問題 7 中提到有 CCD 坡面畫面等資料作為取代。
7.	選擇之研究區域其資料是否足夠完整及充足？本署針對大規模崩塌有多處監測亦有 CCD 坡面畫面等資料，或可參考。	感謝委員的建議與指導，若可取得水保署針對大規模崩塌之監測資料及 CCD 坡面畫面資料，我們便會重新評估資料品質、位置、及數量，若選定之研究區域資料量較小，即配合所取得之資料進行使用。
二、	有關計畫書格式及經費審查部分：	
1.	本計畫請以補助經費584仟元調整編列。	遵照辦理。

項次	審查意見	回覆辦理情形
2.	本年度執行期限請修正為自113年2月7日至113年12月31日。(10.9個月)。薪俸、保險、退休離職儲金、主持人費、兼任研究助理，請以計畫執行期限10.9個月內編列。年終獎金亦配合計畫期程。	遵照辦理。
3.	「按日按件計資酬金」請說明量化，總金額應低於業務費之35%。	遵照辦理。
4.	附表一僅提列主持人費即可。	遵照辦理。
5.	創新研究計畫不得採購資訊設備，請刪除。	遵照辦理。

附錄二、期中審查會議紀錄暨回覆辦理情形

項次	審查意見	回覆辦理情形
報告內容審查意見：		
一、	為配合本署業務需求，計畫內容建議調整(或納入後續執行評估參考)部分：	感謝委員建議，將於報告書內容進行調整。
1.	本計畫強調將多種異質資料整合，建立更加準確的崩塌潛勢預測模型。採用的方法是聯邦學習法 (Federated Learning)。	感謝委員，本計畫將嘗試應用新穎的聯邦學習法於崩塌判斷。
2.	輸入的模型資料僅考慮地形(坡度與坡向)以及雨量而已。目前本研究沒有考慮地層強度資訊，即便是地質分類也沒有，例如說土壤層或是岩層。還是說本研究假設丹大林道都是變質岩區？而且地表覆土層不厚？即便是變質岩也有板岩、千枚岩、片岩之分，這些都不考慮嗎？葉理面的位態不需考慮嗎？還是說葉裡面的位態就由坡向來包括	感謝委員建議，後續研究將會加入些靜態因子，期望能提升研究成果；惟研究初期在資料的蒐集上面臨較大的挑戰，有鑑於部分地表分類已經將崩塌事件發生的地方標籤為崩塌地，而細部的岩石岩體分類資料取得較為不易，目前本研究增添中央山脈區域作為新的研究區域，並將區域範圍增加，嘗試利用資料量增加的方式讓模型

項次	審查意見	回覆辦理情形
	進去了？	能夠學習到區域內的複雜映射關係。
3.	其中報告書對於期中以前的成果呈現，太過於簡略了！僅僅不到一頁的文字來說明，而且沒有任何的圖表。	感謝委員指導，聯邦學習於此領域之應用屬於較為新穎的嘗試，在模式建置前對於國內外文獻全面的蒐集整理，以及因為資料網格解析度關係的資料處理，花費較長時間，本研究已經於期中報告繳交後，進行模式建置，目前模式成果也增添於報告書當中，目前亦持續發展、提升模式效能；惟新模式的發展，要能一蹴即成並非容易之事，要在此計畫期程內將模式發展成熟，是有其困難度，然本研究團隊仍將戰戰兢兢、克服問題、努力專研，期未來能持續得到貴署的支持，發展一套屬於台灣本土且高效能的新穎崩塌預測模

項次	審查意見	回覆辦理情形
		式。
4.	Page 1-4, 「...進行模型建構, 建構完成後以聯邦學習方式設定模型學習輸入資料與崩塌的映射關係, 最終建立防災預警系統」, 請問如何由此兩項「設定模型學習輸入資料」、「與崩塌的映射關係」來建立防災預警系統? 方法論為何?	感謝委員, 目前是嘗試應用聯邦學習技術, 試驗是否可以改善模型抓取崩塌事件的能力, 以單一模型來說, 僅僅只靠該區域目前的輸入資料特徵數是無法對崩塌事件進行有效的預測的, 而後續加入聯邦學習後, 模型在抓取崩塌事件的能力上確實有改善, 透過聯邦學習將邊緣端模型的神經元權重重新聚合, 實現可以更普遍化抓取崩塌事件的模型產出。但此處描述, 確實需要修改, 報告書已改為: 「...進行邊緣模型(Edge model)建構, 多個邊緣模型建構完成後, 將以聯邦學習概念整合多個邊緣模型之訊息, 建立輸入資料與崩

項次	審查意見	回覆辦理情形
		塌的映射關係，嘗試利用聯邦學習之高效能表現，建置於防災預警系統」
5.	針對審查意見 4 之回復，聯邦學習法異質資料之間的「權重整合(weight aggregation)」在本研究中如何具體落實？坡度、坡向、雨量等要分別給多少權重？	權重聚合以 FedAVG 演算法作為聚合的方式，其中所指的權重為每一個邊緣端模型內部的神經元經過資料輸入進行模型訓練後，都會產生它專屬的權重，而演算法會將每一個邊緣端模型的權重提取出來聚合進入中央模型，讓中央模型能夠得到告為普遍化的預測能力。
6.	第四章結論突提及準確率 80%，這是表示好嗎？還是不好？崩塌常因水文事件觸發，換句話說，「雨下在哪裡？大概崩塌就在那裏。」所以水文因子掌控，即便是用深度學習來做多重的卷積、類神經網路計算，也大概就是反映出水文因子。	感謝委員，本研究為嘗試引入新的方式於崩塌預測，因此主要先以常見的資料先進行分析、模型建構，目前以會觸發崩塌事件發生的坡度、坡向及累積雨量為主；準確率 80%是模型抓取崩塌加上未崩塌的總數，但目前在抓取崩塌事件的表現上，還有

項次	審查意見	回覆辦理情形
		很多改善空間，但本研究也有些初步結果，如僅用邊緣端模型，經由現在的輸入資料，是無法對崩塌事件進行有效的抓取，結合聯邦學習的概念還是能夠提升模型效能；待後續持續深入探究，定能建置出高效能之模式。
7.	雖此為嘗試性研究，但以目前呈現的期中成果文字與第四張「未來中長期的建議」內容來看，離可應用階段還有段距離。	感謝委員，目前已確認是否可以透過聯邦學習的方法捕捉到崩塌的發生，改善機器學習受限於特定的資料區域所帶來的侷限性，針對資料稀少的地方也可以進行崩塌的預測；然誠如上述回覆，新模式的發展，要能一蹴即成並非容易之事，要在此計畫期程內將模式發展成熟，是有其困難度，然本研究團隊仍將戰戰兢兢、克服問題、努力專研，期未來能持續得到貴署的支持，發展一套屬於台灣本土且高效能的新穎崩

項次	審查意見	回覆辦理情形
		塌預測模式。
8.	本案以2021年南投縣丹大林道崩塌為試區，其中6月23日較為顯著，惟新增崩塌分布範圍是否涉及道路邊坡請提出說明	感謝委員，後續實施發現丹大林道的崩塌事件量不足以讓聯邦學習有好的表現，因此我們將研究區域轉移至崩塌發生較多的中央山脈區域進行邊緣端模型的建置，並針對南迴公路區進行測試，相比於丹大林道，模型的表現有所提升。
9.	雖模型結果預測準確率(Accuracy)達到85%，惟未崩塌事件數量大，作為模型目標訓練區域崩塌事件數過少，是否在參數上或其他方式加強訓練。	感謝委員建議，未崩塌事件的佔比於資料的總量來說非常大，因此我們重新選取建置客戶端(邊緣端模型)的區域，盡可能篩選崩塌事件較為頻繁的中央山脈某些特定區域作為邊緣端的資料集，其資料的崩塌比未崩塌皆約為 2：8，盡可能讓邊緣端模型能夠從資料學到崩塌與輸

項次	審查意見	回覆辦理情形
		入的映射關係，目前成果已描述於報告書。

附錄三、期末審查會議紀錄暨回覆辦理情形

項次	審查意見	回覆辦理情形
委員審查意見：		
1.	本研究以坡度、坡向及 2 日累積雨量為模型輸入因子，並以 2021 年崩塌事件為比對資料，其網格單元採用 20mX20m，因為崩塌形狀並不固定，對於固定網格面積中其崩塌所佔比例不同，該如何標記該網格為崩塌或未崩塌。	感謝委員，在重新標籤作業中，本計畫將原始崩塌資料的 shapefile 檔案匯入 ArcGIS 軟體，並將其轉換為 20 公尺的矩形網格單元，標記結果如報告書內圖 6 所示，其中黑色區塊為崩塌區域。標記完成後本計畫針對網格單元問題設定兩種不同任務，說明如報告書內頁 2-23，回歸任務為將崩塌標記回推至 1 公里網格單元（圖 6 中的灰色格子），以此計算各大單元內的崩塌機率，而分類任務為純粹判斷 20 m 網格單元是否崩塌。
2.	本研究是以坡度、坡向及 2 日累積降雨量為特徵值，其所訓練出之預測模型，是否能回饋在多少坡度區間、坡向方	感謝委員的指導，在未來研究，我們將持續優化模型，使其能精確地針對崩塌比例較高的區域進行分析，並設定

項次	審查意見	回覆辦理情形
	向、及降雨量區間下易發生崩塌事件。	相關的輸入參數範圍進行回饋展示，例如坡度、坡向以及累積雨量的區間，並將結果以易於閱讀的形式表現，供相關單位參考。
3.	本研究的崩塌潛勢預警系統在實現即時更新與高效預警上，預測模型藉由定期更新氣象與地質數據，進行網格崩塌風險評估，因目前ROC-AUC為0.66，後續是否需在重新進行模型訓練。	感謝委員的指導，本計畫中，ROC-AUC 結果（圖 18）顯示的結果為 ANN 模型的表現；目前，我們已更換為 CNN 模型進行訓練，同時將訓練目標由原本的二元分類（是否發生崩塌）調整為預測大網格單元內的崩塌機率，此更換的主要原因是雨量網格資料與崩塌資料的網格大小存在較大差異，比較更換模型後的結果顯示（圖 20），CNN 模型展現出更佳的預測能力。