經濟部 109 年度

《次世代物聯網關鍵技術與應用系統淬鍊計畫》

合作研究計畫

《雲霧協作架構之分散式聯邦學習(Federated Learning)的運算研究計畫》

建議書徵求文件

財團法人資訊工業策進會

中華民國 109 年 03 月 18 日

109 年度合作研究計畫建議書徵求文件

一、 簡介

近年來由於深度學習技術的發展與應用，帶動了一波人工智慧的浪潮。無論是在醫療、製造、交通、金融、農業等領域，都已有許多成功的案例，吸引許多企業與公司積極導入深度學習技術並開發人工智慧產品，也開啟了嶄新的人工智慧市場與商機。但為了能夠訓練出更準確的深度學習模型，人們不斷提升模型的複雜度，因此需要更大量的訓練資料以及計算資源。目前常見的方式大多是在雲端系統架構下，將資料蒐集儲存後，利用雲端資源從中萃取分析有價值的資料，或是建立訓練模型。但如今這種雲端的架構也逐漸面臨到瓶頸，包括大量的數據可能會造成網絡的壅塞、數據中心的嚴重負擔、以及增加安全上的漏洞。尤其在許多應用上(如醫療、製造)，資料具有高度的隱私性，甚至不被允許上傳至第三方的雲端系統。這些問題已成為深度學習進一步發展的最大阻礙。

為了解決傳統集中式模型訓練下產生的資料收集與隱私問題，「聯邦式學習(federated learning) 」在近年被提出，並逐漸受到重視和採用。所謂的「聯邦式學習」就是一種能夠實現在資料分散且不共享的計算環境與限制下，進行深度學習模型訓練的計算方法。利用聯邦式學習有兩三好處：第一是資料的隱私可以被確保，因此可以吸引更多的使用者提供訓練的資料，共同參與模型的訓練，提升模型的訓練準確度。第二是避免了資料收集過程所產生的網絡壅塞以及時間延遲，提升訓練的計算效率。第三是利用使用者端、或是資料收集的邊緣裝置進行部分的模型訓練計算，減少雲端的負荷。尤其隨著物聯網世代的來臨，邊緣裝置的計算能力日與漸增，有效利用這些閒置的計算資源，更可以大幅降低模型訓練的計算成本。

目前Google已利用聯邦式學習方法，開發了一套在手機上預測手寫辨識的產品，驗證了聯邦式學習的可行性與價值。學界也開始研究開發各種可以提升模型準確度、或減少計算資源與時間的聯邦式學習演算法。因此聯邦式學習無疑是未來將深度學習應用擴展到邊緣計算裝置、並且實現跨地域、跨使用者、甚至跨應用的關鍵技術。

二、 計畫目標

如今聯邦式學習方式與技術還在剛起步的階段。一方面在模型訓練的方法設計上比傳統模型訓練的方法更加多樣化和複雜。由於邊緣裝置的網路頻寬、計算能力、甚至可用性都可能隨著時間和地點有所改變，不僅需依照應用環境中的硬體限制與系統架構做調整，還需隨著邊緣裝置各自收集資料的數量、品質、內容上的差異而有所調整。另一方面如何將設計出計算方法實現在真實的邊緣計算環境也是一大挑戰。由於邊緣裝置各自擁有不同的計算能力，網路連結的頻寬較不穩定，要在變動且不穩定的計算環境中達到可靠的計算服務就有其困難度。為了解決上述困難、加速模型的開發，人們必須依賴如TensorFlow、PyTorch的計算框架。但不幸現今的深度學習計算框架，都是針對傳統集中式的計算環境和訓練方式所設計，並不適用於邊緣計算的環境或聯邦式學習的計算方法。因此本計畫的目標就是要開發一套可運行在邊緣計算環境上的聯邦式學習計算框架。讓模型開發者可以透過此計算框架設計開發不同的聯邦式學習計算方法，並讓模型開發者能直接在真實的邊緣計算環境中做模型的測試優化，加速實現基於聯邦式學習的深度學習解決方法。

三、 計畫範圍

於雲霧架構下，開發能利用邊緣運算裝置及分散資料，進行聯邦學習模型訓練與推論的計算框架，並設計最佳化模型訓練的學習演算法。

四、 預期成果(明確說合作研究成果之產出)

1. 系統架構設計：本畫研究針對深度學習計算之雲霧協作平台，產出成果將包含運用聯邦學習(Federated Learning)在邊緣運算架構下進行分散式機器學習訓練與推論之計算方法設計與計算框架。
2. 專利概念：將完成一項本研究果之專利概念提案，予資策會未來可提出申請。
   ※前述成果如有專利構想或專利申請產出時，需注意專利申請之新穎性(novelty)。因凡經公開發表之研發成果，如擬申請專利，須於公開發表後6個月內完成，前述成果如是以論文方式公開發表，將無法取得大陸與歐盟等國之專利。

五、 執行方式 (包括計畫時程、計畫分工方式)

1. 109年06月30日前交付期中研究報告一篇與成果原始程式碼及其說明文件一份。
2. 109年07月31日前運用聯邦學習(Federated Learning)在邊緣運算架構下進行分散式機器學習訓練與推論之運算技術，並提出至少一個專利構想。
3. 109年11月30日前交付期末研究報告一篇與成果原始程式碼及其說明文件一份。
4. 109年12月15日前進行期末計畫成果之教育訓練。
5. 於計畫執行期間，不定期與本單位就計畫內容及研究範圍進行討論。

六、 計畫期程及預估計畫總經費

計畫執行區間： 109 年 01 月 01 日 至 109 年 12 月 15 日
總經費： 800,000 元

七、 驗收標準(含教育訓練)

1. 「雲霧協作架構之分散式聯邦學習(Federated Learning)的運算研究計畫」期中研究報告1篇
2. 「雲霧協作架構之分散式聯邦學習(Federated Learning)的運算研究計畫」期末研究報告1篇
3. 建構並運用Federated Learning在邊緣運算架構下進行分散式機器學習訓練與推論之運算技術，並提出至少一個專利構想
4. 期中及期末計畫成果原始程式碼及其說明文件各一份。
5. 計畫成果之教育訓練

八、 技術能力需求(請詳述所需要之技術能力或專長)

1. 霧運算(Fog Computing)或行動邊緣運算(Mobile Edge Computing)相關研究
2. 物聯網或分散式運算相關研究
3. 演算法設計及分析或最佳化相關研究
4. 深度學習(Deep Learning)與聯邦學習(Federated Learning) 相關研究

附件1：契約書格式
1-1：計畫書格式

1-2：經費動支報表
1-3：成果報告撰寫須知
1-4：報告格式
1-5：論文格式
1-6：保密聲明書
1-7：委託匯款同意書