

基於最佳化技術之高效率與高效能泛用性聯邦學習式演算法暨公平性分潤機制

本院覽號

32A-1130319

公告日期

2024-09-09

智財權狀態

美國臨時案已申請

摘要

本研究構建一項創新聯邦式學習演算法，透過參與者模型權重界定子空間，進而縮小最佳參數搜尋範圍，有助降低聯邦式學習架構中參數傳遞頻率，增進資料隱密與安全保障，擴充訓練資料多樣性，充分善用分散式運算資源，迅速達致模型收斂，有效提升模型訓練效能。具體成果彙整如下：

1. 廣泛適用於各類神經網路模型及其他機器學習演算法。
2. 基於最佳化理論，透過嚴謹數學推演構建完整演算法。
3. 通過最小化模型參數通訊，強化參與者隱私與安全防護。
4. 優化 FedAvg 演算法，並有效降低系統運算成本。
5. 針對 FedAvg 演算法進行優化，提昇系統收斂速度。
6. 適用所有聯邦式學習演算法之場景，實現系統通訊成本最小化。
7. 鼓勵並評估參與者貢獻，提出創新激勵機制與公平商業模式架構與分析。

創作人

蕭邱漢、林永松

技術優勢

- 本專利乃新穎聯邦學習演算法，以參與者模型權重界定子空間，縮限最優參數搜尋範圍，促使全域模型迅速收斂，降低通訊頻率與傳輸訊息量，確保參與者隱私與傳輸資料安全。
- 按照參與者貢獻度構建完善激勵機制，鼓勵高品質資料參與者加盟提昇全域模型效能，本演算法最佳解優於近似FedAvg演算法，並大幅減輕伺服器與參與者端運算資源。

應用範圍

此泛化型聯邦式學習框架可運用於諸多商業領域，包括：金融、醫療保健、生物科技、電信、教育、交通運輸及零售等產業。其可提升用戶體驗例如：智慧推薦、個性化廣告以及參與者分析等面向。此外，聯邦式學習亦可作為物聯網與智慧城市等領域中之一項技術元件，有助企業保障參與者隱私與資料傳輸安全並提供更好產品與服務。



中央研究院
ACADEMIA SINICA