「國外教授來訪學術演講」-Privacy-preserving Machine Learning (II)

時間：2021-01-04
地點：E310

本次「國外教授來訪學術演講」活動邀請 Department of Electrical Engineering, University of South Florida 張致恩教授蒞校演講，演講內容主要為使用機器學習的方式來保護隱私(Privacy-preserving Machine Learning (II))。演講內容主要分享與介紹藉由機器學習來保護資料的方法。講者開頭先介紹一些基礎的機器學習知識並且說明其中的操作原理，之後講者分享了資料外洩之相關案例，舉例說明：如果一間公司在 1 月份時有 100 位員工，而每位員工的平均薪水是 5.55 萬元；2 月份時有 101 位員工，而每位員工的平均薪水是 5.56 萬元，這樣就可能會被有心人士推測出新加入那位員工的薪水，講者進一步的說明，解決方法就是把薪水寫多加一點，讓它變成不是真實的數字，讓外人猜不到新進員工的薪水，但至於要加多少數值則是需要經過一連串複雜的計算。最後活動尾聲，講者勉勵在場聽眾，未來如有想往電機相關領域發展，隨著現今時代的進步與發展，需要時時精進自己的能力才不會被淘汰。



張致恩教授講解機器學習的知識(1)