

用AI「聯邦學習」技術護私隱 已進入實際應用階段

● 科創獻活力

數字化浪潮席捲全球，但亦衍生新型社會挑戰，需要持續透過科技創新應對。二維碼（QR Code）技術自上世紀九十年代發明以來，目前已被廣泛應用於社交媒體、移動支付、產品促銷、物流追蹤、智能城市等場景，成為日常生活不可或缺的一部分。然而，由於二維碼製作簡單，讓不法分子有機會透過偽裝或將含病毒的惡意連結編入其中，令市民蒙受損失。針對這些風險，嶺南大學學者打造防偽二維碼私隱保護技術，利用人工智能（AI）模型的「聯邦學習」（Federated Learning）等多元技術，藉以堵塞藉偽冒二維碼竊取個人私隱資料的漏洞。該技術目前已進入實際應用階段，期望能有效惠及大眾。

●香港文匯報記者 姜嘉軒

——維碼的製作門檻很低，一些不法分子會偽裝成銀行甚至政府部門等機構，向市民發放含有病毒等惡意連結的二維碼，誘使市民點擊進入假網站。使用者一旦掃描二維碼，就有機會導致身份證、銀行賬戶號碼、支付密碼等個人資料遭盜取，最終或被不法分子利用進行未經授權的交易。」嶺大協理副校長（策略型研究）、利榮康計算智能學講座教授鄺得互接受香港文匯報專訪時表示。

他指出，傳統的二維碼技術便捷，但潛藏相關安全隱患，加上其認證依賴雲端（Cloud）中央處理模式，使用者資料需即時上傳至雲端完成驗證，資料如同暴露在公共空間，就如一道「不設防的電子大門」，且使用者在取用資料時，無法揀選適用部分，而是每次都需要將全部資料由雲端移送出來，也增加了時間成本。

針對這些風險，鄺得互率領團隊打造防偽二維碼私隱保護技術，「我們技術的核心，在於運用AI的『聯邦學習』來達成保護私隱的目標。當使用者掃描二維碼時，系統會對二維碼相關資料進行特徵提取，並將這些加密後的特徵數據傳輸至多個參與驗證的地方，協助完成計算與驗證流程。」

無須上傳雲端 防資料遭竊取

他表示，在新機制下的驗證過程中，原始數據始終安全地保留在本地設備中，全程無須上傳至雲端，這極大地降低了資料在傳輸、儲存環節遭竊取或洩露的風險，從源頭上保障了用戶私隱，尤其在處理身份證明、進行金融交易等高敏感度應用時，能大幅提升使用者的私隱保障。

此外，在實際使用二維碼時，常常會受到污漬覆蓋、圖像折疊導致模糊，或者因拍攝角度不佳、光線過強過暗而扭曲變形等因素干擾，令識別準確性大打折扣，更有可能被不法分子利用模糊、扭曲的偽造二維碼來躲避傳統識別系統進行欺詐，「因此新技術採用預先訓練的視覺變換器來顯著提升驗證準確性，當面對模糊或扭曲的二維碼時，視覺變換器能憑藉自身機制，聚焦於二維碼中的關鍵特徵區域，有效排除干擾資訊，以準確識別出二維碼內容進行影像辨識，確保在複雜情況下也能穩定、準確地提取關鍵特徵完成驗證，保障了交易和驗證的暢順運作。」

可獨立追蹤「商品身份」 貴價品受惠

在防偽功能方面，鄺得互團隊提出了「一物一碼」的創新概念，包括不允許透過影印或使用手機拍攝二維碼等方式進行二次使用，確保每個二維碼的獨一無二，即使是生產商也無法重複使用同一個二維碼，他說：「這樣的措施不僅能有效防止偽冒二維碼的出現，還能為用戶提供更高的安全保障。」

通過實現「一個二維碼追蹤一件物品」，能使每一件「商品身份」都能被獨立追蹤，特別適用於有較高偽冒風險的商品，例如名貴首飾、手錶等高價產品，使用者可以輕鬆驗證商品的真實性，並隨時追溯其來源和歷史。

除可應用到產品防偽之外，鄺得互預計此技術可應用到不同場景，例如在版權保護領域，可保護電子書、音樂、電影等內容版權；在食品安全上，消費者透過掃碼就能獲取食材來源、生產日期、保質期等訊息；金融行業可用於電子收據、支票、銀行卡等金融產品的防偽；在電子票務與門票管理方面，觀眾在大型演唱會、體育賽事均可通過二維碼門票快速驗票入場，防止「黃牛」假票的出現。

鄺得互說，經過團隊就AI模型開發與反覆測試，技術已進入應用階段，團隊正與香港和內地工商界企業及相關機構深入溝通，就技術合作等探討具體方案，將私隱保護、安全驗證等核心功能擴展至中小企業和大眾生活中。



嶺大創防偽二維碼「禁翻兜」



▲鄺得互的「防偽二維碼私隱保護技術」，早前獲第五十屆日內瓦國際發明展銅獎。受訪者供圖

▲鄺得互表示，經過團隊就AI模型開發與反覆測試，技術已進入應用階段。受訪者供圖

假二維碼詐騙個案

例子1:通訊軟件賬戶認證

- 如用戶在其他裝置登入通訊軟件的網頁版，可透過智能手機掃描二維碼來認證身份。過去曾有騙徒在網上搜尋器，以廣告形式把假冒通訊軟件網站連結置頂，若用戶點選假網站並掃描其偽冒二維碼作認證，其賬戶便有機會被騎劫，由騙徒掌握及與受騙用戶的親友對話，以騙取金錢

例子2:網購貨品

- 網購貨品時，包裹外或會貼上二維碼來儲存貨品資料及方便運送。不過，接收者需要留意該二維碼會否已遭竄改，否則一旦進入偽冒網站便有機會招致損失。消費者若需要查詢貨品詳情，建議直接翻看該訂購網站或應用程式內的電子訂單資訊，以免衍生Quishing（QR網路釣魚）的風險

例子3:停車場繳費

- 英國的停車場和電動車充電站均曾出現虛假二維碼騙局。若駕駛者因虛假二維碼連至詐騙網站，其繳款可能被騙徒接收而被停車場罰款，甚至在詐騙網站與騙徒分享賬號和繳費資料，或洩露重要的個人資料

例子4:欺騙善款

- 針對善信捐款，有不法之徒曾將廟宇的捐款二維碼換成個人收款編碼，藉此騙取信眾。事件說明二維碼有機會被輕易轉換，而民眾利用二維碼捐款後，未必會馬上辨認收款人的賬戶和身份，警戒心需要提高

資料來源：香港消費者委員會

使用二維碼小貼士

風險及影響：

- 由於使用者無法直接閱讀二維碼所載的資訊，在掃描二維碼時可能會被連接至惡意網站，因而把惡意軟件下載至流動裝置
- 若不適當使用二維碼進行流動支付，個人資料、交易內容或付款資料可能會遭盜取
- 使用者可能會被不法之徒利用進行未經授權的交易，因而蒙受金錢損失

保安小貼士：

- 掃描二維碼前要提高警覺，確保來源可靠
- 關閉二維碼掃描應用程式中的「自動開啟網站」或同類設定。在關閉此設定後，每次你掃描二維碼時，掃描應用程式都會彈出所對應的 URL，待你確認後才會連接至該網站
- 檢查由二維碼轉化的資料是否正確。如果是網站 URL，小心檢查網站域名是否可信
- 不要隨便向他人透露流動支付服務所產生的二維碼
- 如使用二維碼進行流動支付，小心核實應用程式提供的交易資料，並在完成流動支付交易後，立即核實銀行或流動支付服務供應商發出的交易紀錄

資料來源：特區政府資訊安全網

指港擁優勢與機遇 學者倡加碼研 AI

特區政府近年積極支持創科發展，尤其全力發展人工智能（AI）作為香港的關鍵產業。作為AI領域的專家，鄺得互認為香港擁有多項優勢和機遇，並肯定特區政府對創科研究的支持力度正不斷提升。他期望政府和企業能繼續加大對AI研發的投資，促進更多創新科研合作，同時釐清AI技術的發展與應用藍圖，以充分發揮其潛力和優勢。

鄺得互表示，香港擁有多所世界級知名大學，廣納全球頂尖人才，學術及研究成果豐富，特別是在AI和數據科學等領域表現突出，能幫助香港在學術領域發揮引領作用，培養大量研究型專才，亦為AI技術發展提供寶貴的人才庫。

他分享道，嶺大的目標是成為數字時代領先的文理融合型大學，培養學生掌握運用大數據和AI的技能，遂於去年分別成立嶺南高等研究院及數據科學學院，前者由諾貝爾物理學獎得主丁肇中教授擔任榮譽院長，旨在引入來自不同學科的全球頂尖學者，促進跨學科合作，將先進數字技術與全人教育結合；後者由三個學部組成，分別為人工智能學部、工業數據科學學部、嶺南教育機構陳斌博士數據科學研究

所，全力促進跨學科協同創新。

資本市場可為研究提供融資支持

另一方面，香港作為國際金融中心，鄺得互指，資本市場可為AI創新研究提供必要的融資支持，亦便於與內地及世界各地進行科研合作，促進技術交流，積極推動將研究成果轉化落地。同時，香港的網絡基礎設施相對優越，能支援「重數據化」的技術，這些優勢結合香港的國際化環境，為技術發展創造了良好的空間。

他認為，特區政府積極推動創新科技發展，設立科技園區和孵化器，為初創企業提供支援，更形成了良好的創新生態系統，「這種『產學研』合作模式為城市創科注入新動能，若未來能與內地建立跨境數據流動機制，相關科研發展將會事半功倍。」

在機遇方面，隨著特區政府推動智慧城市建設，鄺得互認為AI技術尤其是在交通和環境管理等領域的應用市場廣闊，同時AI技術若能更多與金融、物流、零售等不同行業跨界合作，亦將帶來新的商機。

●香港文匯報記者 姜嘉軒

新質生產力(製造)協會成立 聚焦「智造升級」

香港文匯報訊 香港製造業總工會昨日舉辦第二屆新型工業化論壇2025，深入探討香港製造業升級轉型之路，同時成立香港新質生產力（製造）協會，旨在推動新質生產力發展為核心，聚焦高科技領域，為國家進一步深化改革推進中國式現代化建設作出努力，並宣布將論壇確立為兩年一度的常態化對話平台，匯聚「官產學研投」各界領袖及精英，搭建交流合作橋樑。

論壇兩場的研討會分別以「迎接十五五規劃新質生產力香港未來發展方向」、「新質生產力賦能香港新型工業化：機遇、挑戰與破局之路」為題，匯聚科技、金融、教育及工業發展等領域人士深入探討香港在「十五五」時期的戰略定位，均認為香港須同步推動傳統工業數位化與新興領域規模化，善用內地市場需求驅動創新閉環。

工業專員:因地制宜拓新質生產力

特區政府創新科技及工業局工業專員葛明在活動上致辭時表示，新質生產力與人民的發展歷程息息相關，創新始終是承載科技革命的核心動能。他指出，創科是香港經濟增長的重要引擎，實現科技創新和產業創新的融合，需要強化科研

成果的轉化和產業化。香港必須把握這個優勢，將香港基礎科研的優勢轉化為經濟發展的優勢，因地制宜發展新質生產力。

香港製造業總工會主席李池英致辭時表示，香港新型工業發展勢頭強勁：2023年製造業及新型工業創造768億港元增加值（佔GDP2.6%），增速達7.6%，印證了科技創新正驅動產業高品質轉型。論壇將每兩年舉行一次，目的是匯聚「官產學研投」五方力量，破解產業化瓶頸的關鍵舉措。她呼籲香港業界把握國家「十五五」規劃契機，以創新開拓智能製造新格局、以綠色引領可持續未來，助力香港深度融入國家新型工業化進程。

新成立的香港新質生產力（製造）協會，將聚焦「智造升級、超級增值、人才策基」三大使命，以技術賦能產業升級，推動AI與綠色科技重塑香港製造。

工聯會立會議員梁子穎任會長

工聯會立法會議員梁子穎擔任會長，副會長有陳鄧源、謝嘉榮、陳立基及鄧展允。陳鄧源在活動上致歡迎辭表示，新型工業化是關乎產業路



●香港製造業總工會昨日舉辦第二屆新型工業化論壇2025。

徑、打工仔發展與香港經濟未來的社會變革，是次論壇實現「官產學研投」五位一體協作模式，與會嘉賓的深度參與、參展機構帶來的創新成果及市民的热情觀展，共同印證香港社會對產業升級的期許。他呼籲社會各界以人文關懷為底色、創新驅動為引擎、團結協作凝聚力量，攜手書寫香港新型工業化新篇章。

現場設有展覽，涵蓋香港製造的初創成果和機

械產品展示，向業界及公眾呈現機械臂、綠色節能環保解決方案、自動化包裝線等創新科技應用。參觀市民讚嘆這些發明，證明香港工業仍有強大生命力，期待未來香港有更多科技發展，融入國家工業化的發展。

除此之外，有年輕創業者仔細詢問創新技術原理，更有家長帶孩子體驗機器手臂自主抓取物品，親身感受「香港智造」的魅力。