

## 【土木系熊貓講座】小數據產生大影響 Roy Maxion籲慎用資料

學校要聞

【賴映秀、記者謝宇晴淡水校園報導】來校擔任熊貓講座的學者卡內基梅隆大學(Carnegie Mellon University, CMU)資訊工程學系教授Dr. Roy Maxion，11月14日上午10時10分於守謙國際會議中心有蓮廳，以他正進行的「分析鍵盤輸入的資訊數據來作個別化識別的研究」實驗，向在場師生展示在實驗室與現場所蒐集的數據比較，因蒐集設備而產生的「壞資料」，其結果可能導致重大的誤判。他也語重心長的告知大家，這些數據所造成的誤判已影響到使用人臉識別的安全系統、醫學，或者法院判決上。他在最後一張簡報中提醒大家，這些不起眼的資料的重要性，小小的數據可能會產生大的影響，並建議謹慎、正確和仔細地篩選數據：「You may forget a few details...but they won't forget you.」。

本場講座由土木系邀請，由國際事務副校長陳小雀致詞開場，並與工學院、AI創智學院兼精準健康學院長李宗翰，及工學院各系主任，和滿座的工學院學生全程參與，Roy Maxion以「When the Rubbish Meets the Road: A Lesson About Data」（當垃圾資料的真相揭曉時：資料的大學問）為題分享他的研究心得，並與在場師生進行意見交流。

Roy Maxion在演說中以他的實證研究展示，如何在雙因素身份驗證的行為生物識別系統中發現數據損壞。他以現在大家輸入密碼作為身分識別為例，「我知道你的密碼，我就可以登錄，我可以成為你。但是，如果我必須以與你相同的節奏輸入它，我就無法這樣做。這就是我們所說的 2 因素身份驗證：其中一個因素是密碼；另一個因素是您輸入密碼的方式。」他以蹣跚步履走向講台中央，表演「步態」，說明在鍵盤上輸入資料，在研究數據的呈現上也同樣具有「步態」，告訴在場師生：「您在鍵盤上自然而然地做的事情，是一種行為生物識別技術，無法模倣。」

他進一步指出，在我們生活之中，看似不起眼的行為動作，都可以透過生物辨識，作為有用的根據，例如人類指紋、打字節奏、行走時步伐，以上舉例都可以透過人工智能系統靈敏度來進行身分驗證。因此，他們對帕金森病患者進行了一項實驗，他們能夠通過他們打字的方式來判斷。他們是否服用了藥物，他們是否度過了美好的一天？他們是否度過了糟糕的一天？疾病趨勢是什麼？他肯定地說：「我們比醫生更了解病人。」

他接著以實驗和現場所蒐集到的資料的比對來說明，「即使 1% 的不好資料，將帶來 16% 的決策閾值差別」，「即使是最小的數據異常也能使發生令人驚訝的變化。」

，而這些小小的數據可能翻轉法院的判決，從無罪變為有罪。

力邀Roy Maxion來校擔任講座的土木系教授范素玲在演講後主持提問，李宗翰、水環系主任蔡孝忠對於資料蒐集方法、經由機器學習是否能模倣人的行為，瞞過生物識別技術？等進行提問與解答。Roy Maxion分享他的實驗室中使用的設備經過非常仔細校準，精確度達到 100 微秒，他以此回答對於數據蒐集的嚴謹態度。至於機器學習雖然能夠輸入相關數據，對於轉化為模仿行為的規格，目前尚未到位，他認為，他所進行的鍵盤輸入研究連輸入者的壓力、心情都能辨識出來，這些都無法經由機器學習模仿。

【潘劭愷淡水校園報導】土木系邀請的熊貓講者，卡內基梅隆大學（Carnegie Mellon University, CMU）資訊工程學系（Computer Science）研究教授Dr. Roy Maxion，11月13日上午10時，由工學院院長李宗翰、土木系系主任洪勇善及教授范素玲陪同，分別拜訪校長葛煥昭及董事長張家宜，葛校長及張董事長分別致贈「熊貓獎座」，及印有李奇茂與張炳煌大師的墨寶、淡江校景及校歌歌詞的花瓶作為紀念。葛校長與張董事長除了對首次來臺的Dr. Roy Maxion致上歡迎及感謝之意，同時也說明本校三化教育理念，及創辦人張建邦伉儷舉~~口~~熊貓講座的由來，並就本次演講主題「When the Rubbish Meets the Road: A Lesson About Data」內容進行初步了解。Dr. Roy Maxion概要說明自己的學術專長，及目前研究的重點方向，透過分析鍵盤輸入資訊數據，以更準確進行個人化識別。他認為單就鍵盤輸入的資訊數據，似乎不足以識別個人，應需要藉由其他方式如個人敲擊鍵盤頻率及力道等特色進行判讀，方能更準確的進行個人化識別，防止因個人密碼遭竊而造成系統的誤判。

Drawing upon extensive experience across diverse domains of AI development, offering consultations to entities such as the U.S. State Department and various industrial and government organizations. His influence extends globally as a guest lecturer at various international universities.

In his past roles, Dr. Maxion served as the Program Co-Chair for the International Conference on Dependable Systems and Networks. He has been a member of esteemed professional organizations, including the IFFF Fault Tolerance Technical Committee, the U.S. Defense Science Board, and the European Commission's AMBER Advisor Committee. Additionally, he contributed to the advancement of security by serving on the editorial boards of prestigious journals such as Transactions on Dependable and Secure Computing, Information Forensics and Security, and Security and Networks. He also served on the editorial boards of IEEE Security and Privacy, and the International Journal of Machine Learning.

淡江時報社

real-world application — user authentication — data corruption was caused by USB keyboards injecting artifacts into the data, effecting an inaccuracy to the true signal. We illustrated how this phenomenon was detected and validated.



淡江  
AI+SDGs=  
ESG+AI=



淡江時報社





