國立中興大學
應用數學系 新聘教師演講

主講人：王紹睿 博士

講題：

Privacy-preserving Data Mining

摘要：

In the era of AI and Big Data, as there is a tremendous amount of data needed to teach and train the AI models, privacy and security have become major concerns. Recently, there are many serious privacy leakage cases of AI companies. For example, in 2016 Google's AI firm DeepMind, which develops the famous AI system AlphaGo, was accused by UK government against their privacy law in the cooperation with National Health Service (NHS); the main reason is DeepMind, without consent, uses the patient's health information, including their HIV reports. Another example is that in 2018 Facebook and a political data-analytics firm named Cambridge Analytica were accused of illegal use of huge Facebook users' personal data for providing assistance and analytics to the 2016 presidential campaign of Donald Trump. For dealing with the privacy issues in AI, especially in the data mining system, in this talk, I will introduce a variety of techniques of Privacy-preserving Data Mining (PPDM), including k-anonymity, ℓ-diversity, differential privacy, homomorphic encryption, etc. Furthermore, I will present my proposed methods, like SOM-Mondrian, DAHOPE, etc., and discuss how these methods overcome the limitation of traditional PPDM schemes, the trade-off between data privacy and data utility. The experimental results show that the proposed methods provide better data utility under the same data privacy level, compared with the previous work.

時間：109 年 7 月 8 日 (三) 上午 11 時

地點：資訊科學大樓 602 室

歡迎本系所師生踴躍參加

國立中興大學應用數學系 敬邀