# 國立台灣科技大學 114學年 第2學期　課程大綱

## Spring 2026 NTUST Course Outline

授課教師：王紹睿

Instructor:Peter S. Wang

課程名稱：隱私資訊安全

Course Title：Data Privacy and Security

2026/11/3

| | |
|---|---|
| 課程代號： CS5164701<br>Course Code<br>學分數： 3<br>Credits | 必選修：選修/半學年<br>Required/Electve:Elective/Half Yr.<br>先修課程：<br>Prerequisites |
| 節次教室：<br>Time/Location | R6(TR-409-1) R7(TR-409-1) R8(TR-409-1) |
| 專業核心能力：<br>Core Professional Competencies | ■具備實驗設計與驗證能力<br>■能發掘並解決問題 |
| 課程網址：<br>Course Website | |
| 課程宗旨：<br>Course Objectives | 本課程主要探討人工智慧(AI)安全領域，特別關注AI系統中的資料隱私問題。課程內容涵蓋以下主題：AI系統(如大型語言模型)可能如何洩露使用者的個人資訊、分散式AI計算框架(如聯邦式學習)中的潛在隱私與安全風險，以及Google、Facebook等主要AI公司如何解決這些問題的技術。在課程中，我們將探討與這些挑戰相關的隱私與安全理論基礎，並介紹各種保護技術，包括隱私去識別化技術Differential Privacy、K-anonymity等，密碼學技術Homomorphic Encryption、Proxy Re-Encryption等，安全多方運算技術Secure Multi-Party Computation。本學期以中文授課，歡迎大二以上選修(提供授權碼)，會先簡單介紹AI和資安的基礎內容。 |
| 課程大綱：<br>Outline of Lectures | Part I. Introduction<br>1. Introduction to Data Privacy and Security<br>2. Introduction to AI/Machine Learning<br>Part II. De-identification Method<br>1. K-anonymity<br>2. L-diversity<br>3. T-closeness<br>4. Differential Privacy<br>5. Local Differential Privacy<br>Part III. Cryptography-based Method<br>1. The basics of Cryptography<br>2. Homomorphic Encryption<br>3. Proxy Re-Encryption and other cryptography-based schemes<br>4. Hybrid method<br>Part IV. Secure Multi-Party Computation<br>1. Secure Multi-Party Computation<br>2. Secret Sharing<br>3. Distributed Computing Applications (Federated Learning, etc.)<br>Part V. Other Recent Issues and Applications: LLM Privacy<br>Part VI. Discussion and final report presentation |
| 授課方式：<br>Method of Instruction | 講授 Lecture：100%<br>分組討論 Group discussion：0%<br>案例研討 Case study：0%<br>操做練習 Practical exercises：0%<br>講授 Lecture：% |
| | |

| | |
|---|---|
| 教科書：<br>Textbooks | *Recent journal & conference papers<br>*S.R. Aravilli, "Privacy-Preserving Machine Learning: A use-case-driven approach to building and protecting ML pipelines from privacy and security threats", Packt Publishing, 2024.<br>*J.M. Chang, D. Zhuang, and G.D. Samaraweera, "Privacy-Preserving Machine Learning", Manning, 2023. |
| 參考書目：<br>References | *Recent journal & conference papers |
| 修課須知：<br>Notice | |
| 評量方式：<br>Grading | *Homework: 60%<br>*Final and Midterm Report : 40% |
| 備註說明：<br>Notes | |