輔仁大學 111 年度 第 2 學期 高教深耕計畫

# 自主學習課程計
# 成果報告書

## 雲端計算概論

授課教師：林振緯 老師
系所單位：資訊工程學系

中華民國 112 年 7 月

# 目次

# 課程規劃

| | |
|---|---|
| 課程實際規劃與說明 | 一、核心能力與目標<br>1. 學生團隊合作<br>2. 學生專題製作與發表能力提升<br>3. 學生自我解決問題能力<br>4. 雲端計畫專業能力再進化<br>5. 專業英文程度提升（需閱讀英文文獻）<br>6. 課程教授內容<br>二、課程簡介<br>1. Introduction to Wireless Networks<br>(1) Computer Networks<br>(2) Wireless Links and Network Characteristics<br>2. Local Area Networks<br>(1) 802.3 Ethernet and the OSI Model<br>(2) 802.3u FastEthernet<br>(3) Gigabit Ethernet<br>3. WiFi 802.11 Wireless LANs<br>(1) The 802.11 Architecture<br>(2) The 802.11 MAC Protocol<br>(3) The IEEE 802.11 Frame<br>4. 802.11 MAC Layer Operations<br>(1) Station Connectivity<br>(2) 802.11 MAC Frame Formats<br>5. Wireless Physical Layer Concepts<br>(1) Frequency Hopping WLANs<br>(2) Direct Sequence Spread Spectrum WLANs<br>6. Secure 802.11 WLANs<br>(1) The Authentication Framework<br>(2) The Authentication Algorithm<br>(3) Data Privacy |

| | |
|---|---|
| 具體教學成果與評估 | 基於課程內容的應用藉由自主學習來實現，以資工、網路相關為主題，來對課堂教學的內容、技術延伸或者是實現，藉由在碩博論文平台與IEEE上查找論文，對於自身一些思考進行實踐或研究來做一個精進，以達到對於未來網路相關的實作部分埋下部分基礎與概念的理解，不光是只學習理論與概念，而是利用實踐來對這門課有更加深刻的學習。 |
| 課程遇到問題與困難 | 1. 主題相關問題：<br>1. 有些組別的自主學習主題與課程較為不同，須選擇與網路相關的主題。<br>2. 自主學習的課程實踐，根據主題亦有難度經由探索與研究來對於網路有更多的概念與想法。<br>3. 主題實作規模過大導致無法在限制時間內達成。<br>4. 挑選的論文品質可能偏差，須審慎挑選論文讀取再研究。<br>2. 報告內容：<br>1. 論文包含主題可能涵蓋內容過大，因考慮報告品質所以只需挑選重點的部分架構去作研究探討即可。<br>2. 對於報告主題的論文熟悉度不足。<br>3. 對論文的焦點偏移，對不是課程主題的內容描寫過多。 |
| 優秀自主學習組別<br>推薦與原因 | 於第三章對於優秀組別進行探討 |

# 2.1.1 課程指導紀錄表

學習助教： 蔡濡謙

| | | | |
|---|---|---|---|
| 時間 | 2023/5/31 | 受指導組別 | 第一組 |
| 地點 | 天主教輔仁大學聖言樓 | 受指導次數 | 第___2___次 |
| 受指導對象 | **柯承佑、陳新義、陳祈叡、張庭豪** | | |
| 指導老師 | **林振緯 教授** | | |
| 指導內容摘要 | | | |
| 主要問題 | 1. 報告的論文內容包含範圍太廣，只需特別琢磨研究單一的主題即可。<br>2. 報告人對於報告的部分內容理解有點生疏，需再熟悉報告內容。<br>3. 實作部分雖然沒有成功，但如果可以分享給聽眾也是不錯的經驗。 | | |
| 具體建議與解決方案 | 專注於部分的重要內容並研究，基本上報告內容都還算了解，只需要再花一些時間熟悉報告內容來減少報告卡住的部分。對於重點部分如果有實際操作部分的描述會更好。 | | |
| 後續追蹤 | 報告一次加強補充部分的內容。 | | |
| 備註 | | | |

*指導紀錄表請自行影印使用

**指導老師：_____林振緯_____**

# 2.1.2 學生自主學習計畫書

一、自主學習計畫主題：Hadoop 雲端運算平台效能模式之評估與改善

二、組別：第一組

三、課程名稱：雲端計算概論

四、指導老師：林振緯

五、學生姓名與工作分配：(可以個人或團體方式執行，至多 5 人)

| 姓名 | 工作內容 |
|---|---|
| 柯承佑 | 選定及閱讀論文、PPT 製作(實驗)、實驗執行 |
| 陳新義 | 選定及閱讀論文、上台報告 |
| 陳祈叡 | 選定及閱讀論文、PPT 製作 |
| 張庭豪 | 選定及閱讀論文、上台報告 |

六、計畫內容與進度規劃 (請描述透過何種行動或方法達成)

我們計畫要探討有關提高 Hadoop 平台效能的論文，並運用論文中使用的技術來實際操作一次，建立一個跨 IaaS、PaaS、SaaS 三層的模型(跨層式參數優化模型，CPOM)，並將「螞蟻演算法」加入模型中，以找出較加參數組合，提高 Hadoop 的效能。

實驗部分則是透過 Hadoop 實際操作來驗證 CPOM 的可行性，確認是否能達到預期效果。

進度規劃如下:

主題選定→研讀論文→資料整理+實驗執行→簡報製作→檢查簡報內容→上台報告。

七、預期效益：

預期能理解蟻群演算法的使用與原理，並準確使用蟻群演算法實現論文內提高 Hadoop 雲端運算平台效能的實驗。以及最終將論文內容分析及整理成老師與同學們都能容易理解的狀態。

# 2.1.3 學生自主學習成果報告

撰寫日期：111 年 6 月 20 日

**一、課程基本資料**

(一)自主學習計畫主題：學習使用 ASP.NET 架設動態網頁

(二)組別：第一組

(三)學生姓名：柯承佑、陳新義、陳祈叡、張庭豪

(四)課程名稱：雲端計算概論

(五)指導老師：林振緯 教授

**二、計畫成果**

(一) 自主學習歷程：

雲端計算的範圍相當廣泛，當初在訂定主題時，我們先決定尋找與課堂中學習過相關內容的論文，並且在簡單瀏覽過找出的多篇論文後，一起決定出一篇最終報告的論文。大家在分工分配及執行上大部分都還算是順利，不過當中也遇到了兩個難題。一個是當初在選定論文時，花了不少的時間。主要是會擔心找的內容會不會太過複雜，超出我們現在程度所能理解的範圍，而導致最終報告的成果不佳。不過還好最終選定的論文中大部分內容都還算在我們能讀懂的範圍內。另一個難題則是原本我們有打算操作論文中最後的實驗部分，並將最終執行結果在報告時呈現，但卻因一些技術方面問題加上最後時間不足而導致實驗最終沒能成功做出來，最後報告時則將這部分改為講解論文作者在文中的執行過程及結果，也是比較可惜的一部分。

(二)成效說明與實際產出：

組員們對於 CPOM 是如何串接 IaaS、PaaS、SaaS 三層，以及如何透過蟻群演算法來找出效能參數並提高 Hadoop 效能有了更進一步的了解。實驗部分，雖然最後沒有成功做出，但也透過文中作者所做的實驗的資訊，了解到該模型確實可以有效率的改善 Hadoop 效能，甚至也可以應用自動化到 Hadoop 叢集上。最終報告時也將我們所理解的內容盡可能的報告給了老師與同學們。

**三、學習心得(組內每位學生皆須提供至少 200 字的學習心得)**

柯承佑:

這是我第一次仔細閱讀完整的論文，也實際透過虛擬機來親自操作 hadoop 平台，我覺得這是一個很棒的經驗。雖然因為時間緊湊的關係我們沒有辦法完整地按照論文的流程做一次一樣的實驗，論文雖然有寫實驗方法及步驟，但是並沒有十分詳細，所以在開始進行實驗時，我在操作虛擬機使用 linux 作業系統時處處碰壁，後來在搜尋大量的參考資料以及教學後才成功，在這之間有獲得很多的

收穫，理解了論文中的概念，並且能夠將其應用於實際情境中。這種實踐使你更深入地理解論文的內容，並將理論知識轉化為實際技能。這樣的經驗對我在分散式計算領域的學習和發展將大有裨益。我已經獲得了寶貴的實踐經驗和問題解決能力，這將有助於我在未來的工作中更加自信和獨立。管在實驗過程中遇到一些困難，這次的學習經驗仍然非常有價值。不僅讀懂了論文，還實際應用了相關技術，並且在解決問題的過程中成長。這個經驗將成為我學術和專業發展的堅實基礎，並為未來的學習和實踐之路鋪平道路。

陳新義:

在這次的自主學習，讓我先對三種系統有了更多的了解，像是 Hadoop 跟 SaaS, IaaS, PaaS，然後了解了他所講述得如何把三種模型建構在一起的想法，透過讀論文，也學習到了不同的演算法是怎麼運作的，包括蟻群演算法跟 Starfish 的介紹以及基本觀念，即使這個專題不是我們自己先開始做的，但是透過研讀他人的結晶也讓我們受益許多，上台的時候也可以多加練習台風，在台上的時候如果去表達你的想法，讓他人知道你在講甚麼，這也是一個學習得地方，跟同組的人一起討論，大家分享對這個論文不同的看法以及認知，在彼此的交流下可以更好的認識這一個東西。而我認為這也是一個很好的自主學習。

陳祈叡:

這次的自主學習，我認為是個相當不錯的經驗。從一開始找論文、研讀論文、怎麼從文中整理出重點並做成簡報，再交給要報告的同學做準備等，的確花費了不少時間，不過也讓我從中學習到了許多。尤其對於平常不會特別找論文來看的我，也有了一次能好好閱讀一篇論文的機會，我認為這些對於將來像是做畢業專題，甚至是未來若讀研究所都是很有幫助的。

透過這次報告，也讓我對於課堂中所提的 Hadoop 及 SaaS、IaaS、PaaS 三層等內容有了更進一步的了解，以及他們彼此之間能如何運用以及結合，來提高 Hadoop 平台效能。同時也從文中多認識了以前沒有聽過的螞蟻演算法等內容，獲得了許多知識。在報告當天，也參考了其他組的同學們是怎麼整理一篇論文內容並做成簡報，最後在台上講解，來思考我們怎麼做可以呈現的更好。這樣的課程安排，可說是獲益良多。

張庭豪:

在自主學習的過程中，了解如何觀賞論文及從中尋找較實用的論文，這是之前比較沒有接觸過的部分，因為要在論文中找出重點及尋找如何運用的方法和上課老師已經整理過的內容相差很多，而且在論文裡運用的技術是我還沒接觸過的東西，在找尋資料與理解的部分花了比較多時間，在實行這個實驗時，也遇到了很多問題，努力了許久找不到解決的辦法，很遺憾，最後的實驗沒有順利完

成，但也讓我們收益良多，之後的人生中也會有很多需要自己學習的時候，經過這次的自主學習，相信之後的路途會比較輕鬆，知道該怎麼應對。

**四、其它附件(必要)**

(一)每組學生成果 PPT

(二)分組討論及相關活動照片


# 2.2.1 課程指導紀錄表

學習助教： 蔡濡謙

| | | | |
|---|---|---|---|
| 時間 | 2023/5/31 | 受指導組別 | 第二組 |
| 地點 | 天主教輔仁大學聖言樓 | 受指導次數 | 第___2___次 |
| 受指導對象 | **陳品璇、吳佳穎、莊綢柔、李維琪** | | |
| 指導老師 | **林振緯 教授** | | |
| 指導內容摘要 | | | |
| 主要問題 | 1. 內容充足、主題明確，但是缺乏核心部分的實現與方法部分的描述，報告中大多講電子發票服務平台的架構，但如何運作的部分需要再補充。<br>2. 無法詳細解釋程式碼運作的功能，需要再花時間研究。<br>3. 應盡量介紹整個系統的模塊分工與各模塊功能讓台下聽眾可以理解。 | | |
| 具體建議與解決方案 | 雖然細節資料很多，但是需要再整理報告內容，尤其是架構部分需要多一點介紹與了解，再介紹細節部分，聽眾才能理解電子發票服務平台的各種網路架構的分工，後續細節才會比較能夠理解。 | | |
| 後續追蹤 | 對於電子發票服務平台架構的部分進行再補充。 | | |
| 備註 | | | |

*指導紀錄表請自行影印使用

**指導老師：_____林振緯_____**

# 2.2.2 學生自主學習計畫書

一、 自主學習計畫主題：論文探討-雲端運算服務導向架構電子發票加值平台和 XML-based 訊息轉換器與資料中心之研究

二、組別：第二組

三、課程名稱：雲端計算概論

四、指導老師：林振緯 教授

五、學生姓名與工作分配：(可以個人或團體方式執行，至多 5 人)

| 姓名 | 工作內容 |
|---|---|
| 陳品璇 | 分析中心控管層資料處理流程、XML-based 資料訊息與轉換和架構 |
| 吳佳穎 | 解析服務供應層之分散式資料庫運作方式及基礎建設層介紹 |
| 莊緗柔 | 整合 XML-based 訊息轉換與資料中心的運作和發票模組介紹 |
| 李維琪 | 統整論文研究問題、歸納解決辦法，解析雲端加值平台架構 |

六、計畫內容與進度規劃 (請描述透過何種行動或方法達成)

先透過閱讀整篇論文的內容對這項主題有一定概念的認識之後，再分配大家的分工內容來讓此次的論文閱讀更有效率，將自己負責的部分研究完成後，在小組討論時再將內容講解給其他人聽，讓大家都能學習到這篇論文中更完整更深度的內容，而非只是一人在短時間下閱讀而忽略了很多地方，也不會有時間不夠去查找相關資料的問題。

七、預期效益：

1. 深入瞭解雲端運算概念：透過對雲端計算概論的學習和研究，我們將對雲端運算的基本概念和原理有更深入的瞭解，包括其架構、運作方式以及在不同領域的應用。
2. 掌握雲端運算與服務導向架構的結合：我們將深入研究雲端運算服務導向架構與電子發票加值平台、XML-based 訊息轉換器和資料中心的結合，並理解其在企業資源管理和融資業務中的重要性和優勢。
3. 學習研究方法和論文撰寫技巧：透過閱讀、分析和討論論文，我們將學習研究方法和論文撰寫的技巧，包括資料搜集、整理和分析，以及如何清晰地表達和呈現研究成果。
4. 團隊合作和提升溝通能力：在小組中進行分工合作和討論時，我們將增強團隊合作和溝通能力，學習如何有效地分享和傳達自己的研究成果，並從他人的分享中學習和吸收更多知識。
5. 提升專業能力和學習成果：通過深入研究和討論，我們預期能夠提升自己在雲端運算和相關領域的專業能力，並獲得實際的學習成果，以應對未來在學術、職業或研究領域的需求和挑戰。

# 2.2.3 學生自主學習成果報告

撰寫日期：2023 年 6 月 15 日

**一、課程基本資料**

(一)自主學習計畫主題：論文探討-雲端運算服務導向架構電子發票加值平台和 XML-based 訊息轉換器與資料中心之研究

(二)組別：第二組

(三)學生姓名：陳品璇、吳佳穎、莊緗柔、李維琪

(四)課程名稱：雲端計算概論

(五)指導老師：林振緯 教授

**二、計畫成果**

(一) 自主學習歷程：（請回顧整個自主學習之執行步驟，摘要寫出歷程）

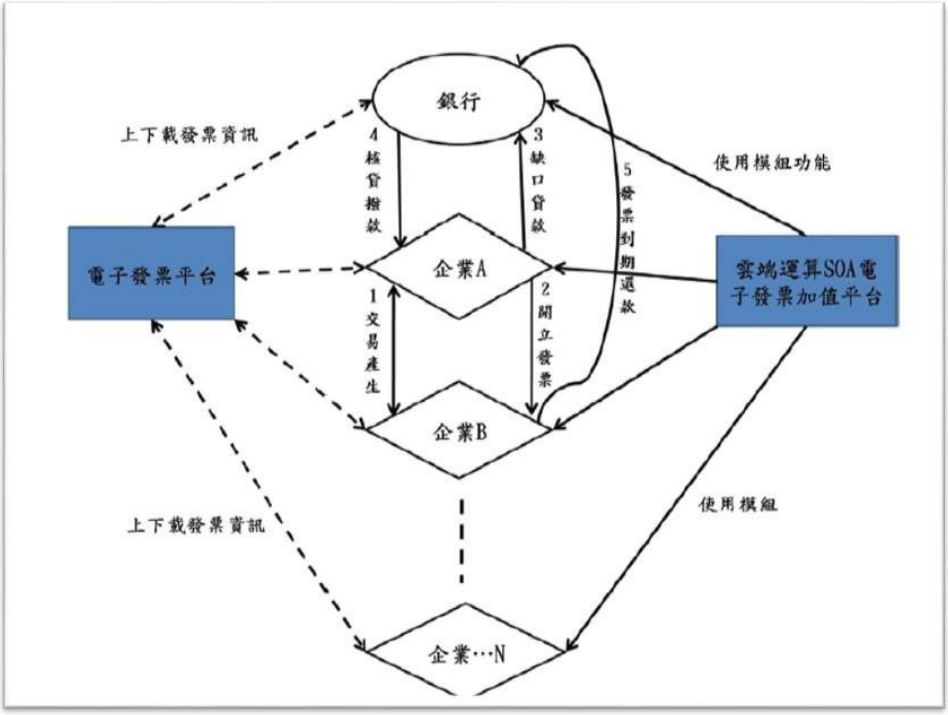
小組中的每個人在台灣碩博士論文的網站中分別尋找跟課程內容有相關的論文主題，並加以討論大家對哪一類雲端導向的應用主題較有興趣，最後我們選擇了實際應用在電子商務環境下的電子發票加值平台和 XML-based 訊息轉換器與資料中心作為我們探討的論文主題。論文的內容不但多又雜，單靠一人閱讀過後來做分享既耗時又無法讀的透徹，所以我們分配了每個人需要分工的任務內容，並按時的完成自己負責的部分。我們將論文大致拆成研究方向、解決辦法、系統架構和應用的技術解說，在大家的努力下，我們都把自己被分配到的區域讀熟，並找到相關的資料加以延伸，最後再跟其他組員們講解、說明，讓大家可以最有效率的讀完一篇論文。但因為是我們從未接觸過的技術，所以在理解這篇研究內容時，花了不少時間去了解這些技術到底是如何運作和其他相關的資料來作為我們知識的基礎，讓我們在學習時可以更深刻
的了解、吸收此篇論文想傳達的事物。

(二)成效說明與實際產出：（可附加佐證資料、文書記錄、照片或相關計畫運作情形資料等）

這篇論文所建立的電子發票加值平台結合了雲端運算和服務導向架構，旨在提供企業更安全、高效的資源和加速融資業務流程。這個平台允許使用者透過 Google Sites 使用各種增值服務，並透過 XML-based 訊息轉換器獲取相關資訊。

其中一個主要優點是這個平台為企業帶來了安全的雲端運算資源。這意味著企業可以透過雲端服務來存儲和處理敏感資料，同時享受雲端運算帶來的彈性和可擴展性。這種架構可以幫助企業提升資金調度能力，並加快小額貸款的申請流程。同時，透過使用這個平台，企業可以節省成本和時間，並更有效地管理其財務流程。另外，這個平台採用了分散式資料中心的概念，將資料存放在不同的資料庫中，從而提高了資料的安全性。這種分散的架構可以減少單一點故障的風險，並提供更高的可用性和容錯能力。

論文提到，透過這個平台和轉換器，企業和銀行之間可以進行更便捷的商流和金流訊息交換。這意味著企業可以更快速地與銀行進行交互，加快融資業務流程。同時，這個平台還提供整合性的加值服務方案，為企業創造更高的附加價值。這些加值服務可以幫助企業更好地管理
其資金流動和財務運營，從而提高營運效率和競爭力。




**三、學習心得(組內每位學生皆須提供至少 200 字的學習心得)**

陳品璇:

這篇論文對我來說是一個非常有價值和有趣的研究，讓我對雲端運算和電子發票加值平台的概念有了更深入的了解。論文提供了一個以雲端運算為基礎的解決方案，讓企業能夠更有效地進行融資並進行安全的交易。其中 XML-based 資料訊息轉換器引起了我的興趣。它能將企業端的電子發票資訊轉換為不同格式，以滿足不同系統和應用的需求。這種技術在金流和商流活動中非常重要，並且能夠提高資料的一致性和互操作性。

透過閱讀論文，我意識到在電子商務環境中，資料處理和安全性是一個重要的課題，而論文提出的解決方案和技術能夠有效地解決問題。這不僅對我個人的專業發展有所助益，也讓我對資訊管理領域的發展趨勢有了更深入的了解。

吳佳穎:

透過閱讀一篇論文，去深度的理解電子發票雲端加值平台的整套運作流程和其中的技術。通過多次閱讀，我初次了解了整個加值過程的大致流程。然後，我開始深入研究技術部分，特別是 XMLbased 的訊息轉換和分散式資料庫的運作。我在理解技術內容後，努力將其完全吸收，並利用論文中的圖表，轉換成 PPT 並進行報告。

這次的經驗雖然對自己的表現還算滿意，但也我更加意識到自己在準備和呈現報告方面仍有進步的空間。清晰的說明並解析分散式資料庫這項技術在整個加值過程的位置，與其運作的過程。雖然準備了一些重點講稿，但還是有些重點因緊張原因而遺漏了。在未來的報告中，我將繼續努力提高自己的準備能力和演講技巧，以便更好地向觀眾傳達我所學到的知識。

莊綢柔:

以閱讀論文自學的方式是屬於比較近期才開始接觸的型態，所以剛開始在把論文紙本轉為口述報告花了比較多的時間在統整，文字的精簡化但又不過於省略細節、敘事上的流暢性、和整體架構的完整性是我覺得在論文報告的構想上較為重要的三個面向。
這次的領域是雲端服務導向，以生活面切入結合日常交易的應用，從企業到金融業，再從金融業到銀行端的流程，一連串的撥款核銷貸款程序把技術生活化，此外多方生活面技術的運用也對研發領域會有較多想法和使用者需求探索。

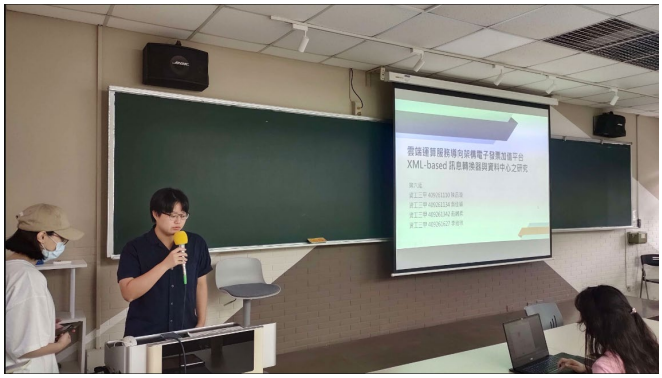
李維琪:

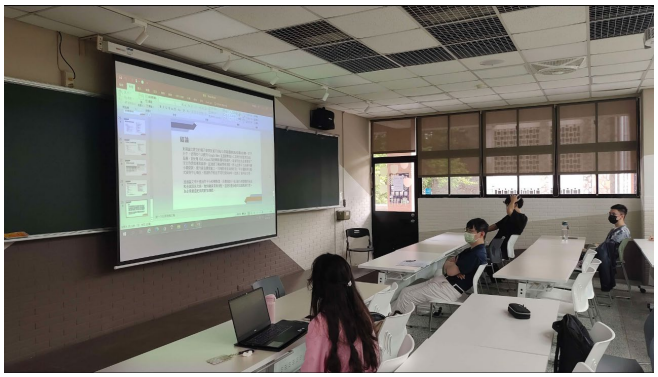
這篇論文介紹了一個電子發票加值平台，該平台結合了雲端運算和服務導向架構，為企業提供了許多優勢和增值服務。我對這個平台的設計和實施感到非常驚訝，因為這個領域是我很少接觸的以外，我還發現原來這些技術竟然能夠在商務領域有很大的發揮，化繁為簡是最不容易的，且這項論文還加了安全性的考量，不但讓企業擁有一個更方便和高效的商流和金流訊息交換平台，也提供了分散式資料中心的概念，將資料存放在不同的資料庫中，從而提高了資料的安全性。這種分散的架構可以減少單一點故障的風險，並提供更高的可用性和容錯能力。閱讀此篇論文不但提升了我對雲端方面技術與知識的概念，也讓我對科技應用到生活有更不一樣的想像。

**四、其它附件(必要)**

(一)每組學生成果 PPT

(二)分組討論及相關活動照片





# 2.3.1 課程指導紀錄表

學習助教： 蔡濡謙

| | | | |
|---|---|---|---|
| 時間 | 2023/5/31 | 受指導組別 | 第三組 |
| 地點 | 天主教輔仁大學聖言樓 | 受指導次數 | 第___2___次 |
| 受指導對象 | **陳文凱、簡煜倫、李睿庭、余穎嵐** | | |
| 指導老師 | **林振緯 教授** | | |
| 指導內容摘要 | | | |
| 主要問題 | 1. 介紹關於網路攻擊的基礎知識，與各種防禦手段，但沒有實際的結果又或者最少該有此篇論文分析這些防禦手段的差異。<br>2. 只是單單介紹 tool，對於 tool 運作的實際方法或者是實現方式沒甚麼介紹。也沒有實作。 | | |
| 具體建議與解決方案 | 需要再補充更多可能關於 tool 的開發與各個防禦手法的差異與效能間的區別，也可能關於論文的內容展現不夠多需要再補充，不然以報告論文來說內容確實有點少。 | | |
| 後續追蹤 | 對每種 tool 差異或者用途細節進行補充。 | | |
| 備註 | | | |

*指導紀錄表請自行影印使用

**指導老師：_____林振緯_____**

# 2.3.2 學生自主學習計畫書

一、自主學習計畫主題：Towards an Applicability of Current Network Forensics for Cloud Networks: A SWOT Analysis

二、組別：第三組

三、課程名稱：雲端計算概論

四、指導老師：林振緯 教授

五、學生姓名與工作分配：(可以個人或團體方式執行，至多 5 人)

| 姓名 | 工作內容 |
|---|---|
| 陳文凱 | 上台報告、論文挑選 |
| 簡煜倫 | 論文挑選、整理資料 |
| 李睿庭 | PPT 主題統整 |
| 余穎嵐 | PPT 主題細節整理 |

六、計畫內容與進度規劃 (請描述透過何種行動或方法達成)

對於網路相關基本知識先有所理解，再了解網路攻擊的各種種類，最後學習論文中一些如何預防與檢測網路攻擊的手段以及一些入侵檢測系統的工具，並進行研究與探討。

七、預期效益：

1. 了解網路攻擊的基礎知識：先理解網路的運作與攻擊方式的基本概念，再學習論文中的一些方式了解如何抵擋網路攻擊事件。

2. 了解網路攻擊模式的基本分類。

3. 了解論文中所描述的抵擋與偵測惡意攻擊的方法。

# 2.3.3 學生自主學習成果報告

撰寫日期： 112 年 6 月 20 日

## 一、課程基本資料

(一)自主學習計畫主題：Towards an Applicability of Current Network Forensics for Cloud Networks: A SWOT Analysis

(二)組別：第三組

(三)學生姓名：陳文凱、簡煜倫、李睿庭、余穎嵐

(四)課程名稱：雲端計算概論

(五)指導老師：林振緯 教授

## 二、計畫成果

(一) 自主學習歷程：

對於網路相關基本知識先有所理解，再了解網路攻擊的各種種類，最後學習論文中一些如何預防與檢測網路攻擊的手段以及一些入侵檢測系統的工具，並進行研究與探討。

(二)成效說明與實際產出：

1. 了解網路攻擊的基礎知識：先理解網路的運作與攻擊方式的基本概念，再學習論文中的一些方式了解如何抵擋網路攻擊事件。

2. 了解網路攻擊模式的基本分類。

3. 了解論文中所描述的抵擋與偵測惡意攻擊的方法。

**三、學習心得(組內每位學生皆須提供至少 200 字的學習心得)**

**簡煜倫**

這篇論文的篇幅非常大，而且還有非常多個人合作。在翻譯論文並整理資料的過程中，我們逐漸學到了如何防止雲端被攻擊的一些重要方法和策略，其中我們 PPT 提到的網路取證方法就包含了許多識別網路攻擊的方法 EX: 通過分析網絡數據包、日誌、應用程序和各種網絡事件，幫助識別、收集、保存、分析和報告來自網絡的數字證據，並調查攻擊的來源。其中的入侵檢測系統我覺得非常實用，因為它不僅可以識別攻擊的敵人源頭，還能預測攻擊者未來可能會發動的攻擊。

**李睿庭**

這篇論文主要是在討論雲端網路會出現的攻擊問題，以及調查這些攻擊的取證方法，SWOT 分析(Strengths, Weaknesses, Opportunities, and Threats)能舉出優勢，弱點，機會，威脅。透過閱讀這篇論文，我學到 NFM 的功能以及不同的類別，NFM 是 network forensics model 網路鑑識，涉及為信息收集、取證證據或入侵檢測目的而監控和分析計算機網絡流量。

入侵檢測系統（IDS）是一種網路安全裝置或應用軟體，可以監控網路傳輸或者系統，在論文中提到一種基於概率和推理機制的分析入侵檢測方法，從安裝在網絡中不同位置的分佈式 IDS 傳感器中檢測入侵警報。因為這次報告讓我能夠了解雲端架構帶來的危機以及監測方法，增加雲端安全的知識。

**余穎嵐**

**為什麼他們會發動網路攻擊？**

網路犯罪每年有增無減，因為有人會嘗試從有漏洞的企業系統中獲取利益。攻擊者經常會要求贖金：53% 的網路攻擊造成了 500,000 美元以上的損失。雲端上的網路攻擊大多是非法訪問、插入惡意代碼、修改封包、竊聽等型態。

為了保護雲端受惡意攻擊，可採取「網路取證」（network forensics）的方法，功能是抓取、記錄和分析網路事件以發現安全攻擊或其他的問題事件的源頭。我們的報告是解釋 C-NFM 的流程，由分析封包（packet）、日誌（log）、應用程序和各種事件來調查攻擊的來源，分成以下四個階段：

1. 入侵檢測：概率推理、模式及協議分析
2. 追蹤：收集網路跡象、匿名通信
3. 分散式：同時在多個不同位置進行分析
4. 攻擊圖：攻擊使用陸路徑、檢測未來可能的攻擊妥善利用科技資源的同時也要懂得保護自身的資訊，為了防止資源因為網路攻擊而使其可用性（availability）、機密性（confidentiality ）、一致性（integrity）遭到破壞、做好網路保護措施是極其重要的。

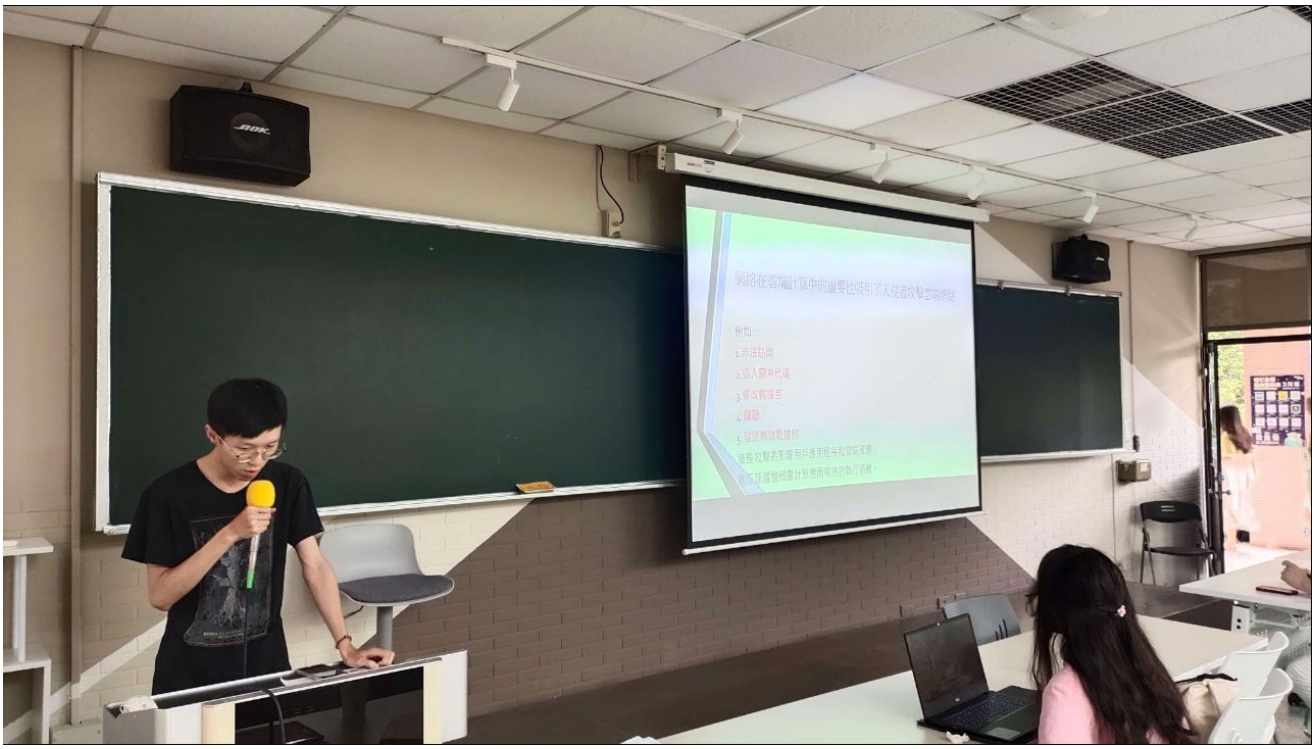
**陳文凱**

做完這次自主學習活動後，了解到網路鑑識是在檢測到攻擊後進行的調查過程。其目標是識別攻擊的根本原因，以便在未來能夠防範類似攻擊。且根據分析，網路鑑識方法分為入侵偵測系統、追蹤、分散式和攻擊圖等四個類別，各有各的優點。入侵偵測系統通過檢測網路攻擊並通知鑑識模塊來分析惡意流量。追蹤方法則用於追蹤攻擊的源頭。分散式方法在網路的不同位置收集並分析網路流量。攻擊圖則用於識別入侵者進行攻擊的路徑。根據這些資訊，網路鑑識為我們提供了多種探索和應對網路攻擊的方法，以保護我們的系統和資訊安全。感謝教授給我們機會讓我們對攻擊及反追蹤手法有更詳細的了解。

**四、其它附件(必要)**

(一)每組學生成果 PPT

(二)分組討論及相關活動照片



# 2.4.1 課程指導紀錄表

學習助教：蔡濡謙

| | | | |
|---|---|---|---|
| 時間 | 2023/5/31 | 受指導組別 | 第四組 |
| 地點 | 天主教輔仁大學聖言樓 | 受指導次數 | 第___1___次 |
| 受指導對象 | **吳家萱** | | |
| 指導老師 | **林振緯 教授** | | |
| 指導內容摘要 | | | |
| 主要問題 | 針對本次專題原主題 - 基於價值最大化資源競爭與物聯網聯邦學習配置策略的整體修改建議，還有就是沒比較兩種算法的差異性。 | | |
| 具體建議與解決方案 | 本次專題主題目標有些發散，可擇其中一項主要問題面向進行問題探討與解決實作。且提出之問題僅偏向理論的演算法教學實作，建議再與實際應用技術結合。 | | |
| 後續追蹤 | 無 | | |
| 備註 | | | |

*指導紀錄表請自行影印使用

**指導老師：_____林振緯_____**

# 2.4.2 學生自主學習計畫書

一、自主學習計畫主題：資源競爭配置最佳化 – 二分圖演算法

二、組別：第四組

三、課程名稱：雲端計算概論

四、指導老師：林振緯 教授

五、學生姓名與工作分配：(可以個人或團體方式執行，至多 5 人)

| 姓名 | 工作內容 |
|---|---|
| 吳家萱 | 主題構想、理論研究、設計模擬實驗並實作 |
| | |
| | |
| | |

六、計畫內容與進度規劃 (請描述透過何種行動或方法達成)

計畫內容：

針對雲端計算之伺服器群集中的資源配置最大化透過二分圖匹配演算法實現進行模擬實驗。

進度規劃：

1. 研究二分圖匹配演算法在資源配置最大化的現有應用。
2. 針對現有二分圖匹配演算法在資源配置最大化的實際架構透過 MATLAB 進行模擬實驗。

七、預期效益：

模擬二分圖匹配演算法在資源配置最大化的實際架構，並探討何種二分圖匹配演算法在資源配置最大化可達到較高效益。

# 2.4.3 學生自主學習成果報告

撰寫日期： 112 年 6 月 14 日

## 一、課程基本資料

(一)自主學習計畫主題：資源競爭配置最佳化 – 二分圖演算法

(二)組別：第四組

(三)學生姓名：吳家萱

(四)課程名稱：雲端計算概論

(五)指導老師：林振緯 教授

## 二、計畫成果

(一) 自主學習歷程：（請回顧整個自主學習之執行步驟，摘要寫出歷程）

1.如何訂定主題？

針對平時上課內容，尋找相關且有興趣之主題領域進行探討研究。

2.分工分配及執行狀況？

執行狀況：

以預期方式實際模擬出二分圖匹配演算法在資源配置最大化的實際配置方式。

3.是否遇到什麼難題？

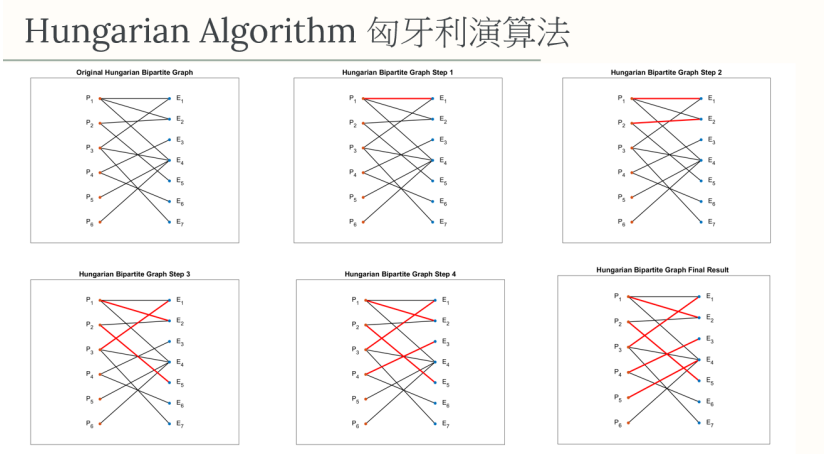
在規劃實驗部分僅以理論實作，應再配合實際應用進行實驗設計。

成效說明：

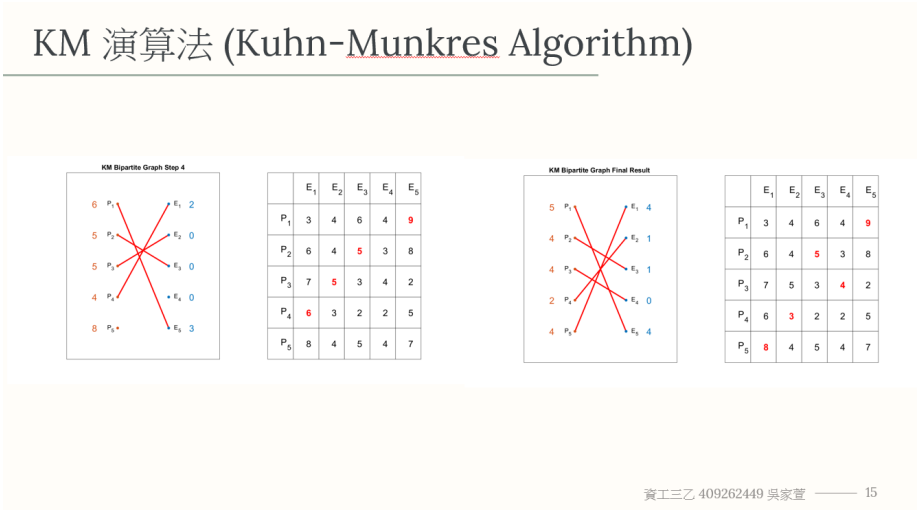
模擬兩種二分圖匹配演算法在資源配置最大化的實際配置方式。

實際產出：

1. 二分圖最大匹配模擬實驗 Hungarian Algorithm 演算法之部份結果輸出圖。




2. 二分圖最大權重匹配模擬實驗 KM 演算法之部份結果輸出圖。




**三、學習心得(組內每位學生皆須提供至少 200 字的學習心得)**

本次的專題研究主題是因受到上課所學習到之伺服器群集資源配置概念的啟發，故想對伺服器群集中的實際架構與工作調度情況更進一步的了解，於是訂了基於價值最大化資源競爭與物聯網聯邦學習配置策略這樣的主題領域方向。

而在期中初報時，老師建議我可以將題目範圍縮小，著重於其中一項技術的向下鑽研精深，以單一技術的展現作為研究目標，避免因主題過於發散而在有限的時間內無法充分學習每項技術以獲得良好的展示。

最終在期末報告時，我將專題主題調整為資源競爭配置最佳化－二分圖演算法，以針對二分圖演算法技術作為資源配置最佳化的主要探討對象，設計兩項二分圖匹配演算法的模擬實驗並實作，但考慮到我設計的模擬實驗較偏向針對此二分圖匹配演算法的理論概念展現，並沒有結合實際應用技術。接下來我期望再利用暑假時間學習如何將課堂學習之理論知識於實際應用技術上。

**四、其它附件(必要)**

(一)每組學生成果 PPT

(二)分組討論及相關活動照片

# 2.5.1 課程指導紀錄表

學習助教：蔡濡謙

| 時間 | 2023/5/31 | 受指導組別 | 第五組 |
|---|---|---|---|
| 地點 | 天主教輔仁大學聖言樓 | 受指導次數 | 第___1___次 |
| 受指導對象 | **邱柏翰** | | |
| 指導老師 | **林振緯 教授** | | |
| 指導內容摘要 | | | |
| 主要問題 | 實驗用的機器基本上只能用我正在用的筆電，那背景程式的執行會影響到實驗結果，該怎麼解決？ | | |
| 具體建議與解決方案 | 只要在建立容器時分配同樣的 CPU 和 RAM，並且在運行時確保主機有足夠的 CPU 和 RAM，那背景程式應該是不會影響到實驗結果。 | | |
| 後續追蹤 | 在實驗中取得了和論文相似的結果，背景程式似乎沒有影響，或是可忽略。 | | |
| 備註 | | | |

*指導紀錄表請自行影印使用

**指導老師：_____林振緯_____**

# 2.5.2 學生自主學習計畫

一、自主學習計畫主題：單體式架構 VS 微服務架構

二、組別：第五組

三、課程名稱：雲端計算概論

四、指導老師：林振緯

五、學生姓名與工作分配：(可以個人或團體方式執行，至多 5 人)

| 姓名 | 工作內容 |
| --- | --- |
| 邱柏翰 | 全部 |
| | |
| | |
| | |

六、計畫內容與進度規劃 (請描述透過何種行動或方法達成)

閱讀論文、翻閱相關書籍和親自實作，主要實作為重做論文的實驗以驗證該論文之結論。

七、預期效益：

了解現今軟體工程上的各種程式架構，並學會設計與實作微服務架構。

# 2.5.3 學生自主學習成果報告

撰寫日期：112 年 6 月 14 日

**一、課程基本資料**

(一)自主學習計畫主題：單體式架構 VS 微服務架構

(二)組別：第五組

(三)學生姓名：邱柏翰

(四)課程名稱：雲端計算概論

(五)指導老師：林振緯 教授

(一)自主學習歷程：（請回顧整個自主學習之執行步驟，摘要寫出歷程）

1.如何訂定主題？

剛好畢業專題在做相關的主題，藉由這個機會先一步地進行習學習。

2.分工分配及執行狀況？

自己一組，沒有任務分工的問題，工作排程良好，都有準時完成。

3.是否遇到什麼難題？

微服務架構通常用在電腦叢集上，但現階段沒有辦法找一個叢集給我進行實驗，所以實驗只在單機上進行。

(二)成效說明與實際產出：（可附加佐證資料、文書記錄、照片或相關計畫運作情形資料等）

我進行的實驗再次驗證了論文中的一小部分結論，單體式架構在單機環境下有著比微服務架構更好的效能，透過這個結果可以得知軟體架構並沒有絕對的優劣，每種狀況都有著最適合的軟體架構，不應該因為微服務架構的嶄新與大型企業都在使用而過度追捧。

**三、學習心得(組內每位學生皆須提供至少 200 字的學習心得)**

這次的自主學習讓我體驗了一次研究所的生活，從讀大學以來第一次去看英文論文，雖然沒有什麼艱辛的語法，但眾多看不懂的專有名詞也是令我苦不堪言，但花時間了解論文的主題與動機後，也能理解作者的實驗為什麼那樣設計，後續實驗結果的討論也非常有意思，提出了很多我沒想過的觀點，讓我受益良多。

而實作上我也學到了如何操作 Apache JMeter 進行壓力測試和建立容器化程式，雖然耗費了大量時間研究 Docker 如何運作才勉勉強強做出一點實驗，但在我了解容器之後我認為這一定是值得的，容器優秀的設計注定成為未來主流的部署方式，所以花上再多心血都很划算。

**四、其它附件(必要)**

(一)每組學生成果 PPT

(二)分組討論及相關活動照片

交付在提交報告 Word 裡面

# 2.6.1 課程指導紀錄表

學習助教：

| | | | |
|---|---|---|---|
| 時間 | 2023/5/31 | 受指導組別 | 第六組 |
| 地點 | 聖言樓 | 受指導次數 | 第___2___次 |
| 受指導對象 | **陳席偉、林宇恩** | | |
| 指導老師 | **林振緯 教授** | | |
| 指導內容摘要 | | | |
| 主要問題 | 針對一項有運用結合 MEC 與雲端運算於車載網路中有效路徑規劃這篇論文做研究，並且上台報告。 | | |
| 具體建議與解決方案 | 要有 MEC 和 RSU 的架構圖並解釋。 | | |
| 後續追蹤 | | | |
| 備註 | | | |

*指導紀錄表請自行影印使用

**指導老師：林振緯**

# 2.6.2 學生自主學習計畫書

一、自主學習計畫主題：結合 MEC 與雲端運算於車載網路中有效路徑規劃

二、組別：第六組

三、課程名稱：雲端計算概論

四、指導老師：林振緯

五、學生姓名與工作分配：(可以個人或團體方式執行，至多 5 人)

| 姓名 | 工作內容 |
|---|---|
| 陳席偉 | 講解內部所使用的演算法。 |
| 林宇恩 | 講解整體架構。 |
| | |
| | |

六、計畫內容與進度規劃 (請描述透過何種行動或方法達成)

閱讀論文，上網針對特定名詞找資料。

七、預期效益：

了解各個裝置之間的關係，和演算法法的運用。

# 2.6.3 學生自主學習成果報告

撰寫日期：2023 年 6 月 15 日

## 一、課程基本資料

(一)自主學習計畫主題：結合 MEC 與雲端運算於車載網路中有效路徑規劃

(二)組別：第六組

(三)學生姓名：林炫宇、林俞駿

(四)課程名稱：網路概論

(五)指導老師：林振緯

## 二、計畫成果

(一) 自主學習歷程：（請回顧整個自主學習之執行步驟，摘要寫出歷程）

1.如何訂定主題？

在論文網站找出自己感興趣的主題。

2.分工分配及執行狀況？

分成架構和演算法兩個部分，一人講解一個

3.是否遇到什麼難題？

退火演算法，以前沒有聽過，要重新理解。

(二)成效說明與實際產出：（可附加佐證資料、文書記錄、照片或相關計畫運作情形資料等）

Cloud內模擬退火演算法
求近似最佳解

1.初始化：設定初始解以及初始溫度和終止溫度，最大迭代次數。

2.生成鄰近解：用函數於為當前解產生一個新解

3.接受或拒絕鄰近解：根據接受機率，決定是否接受鄰近解。

4.更新溫度：降低溫度以找尋別的鄰近解。

5.檢查終止條件：檢查是否達到最大迭代次數。

6.返回最佳解：返回最佳解。

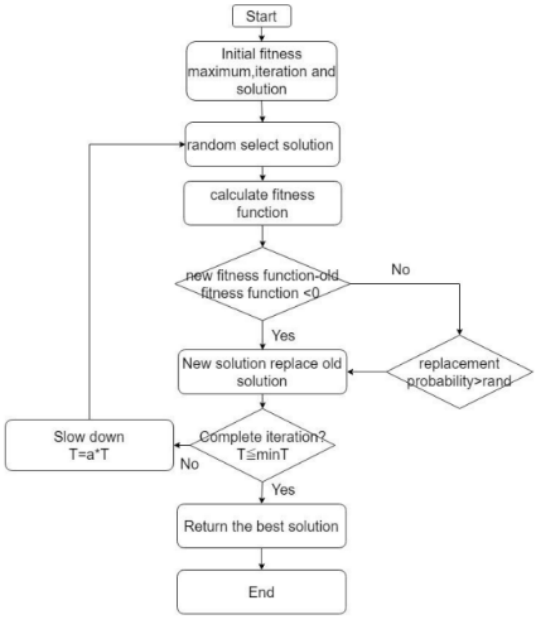



圖 4：模擬退火演算法流程圖

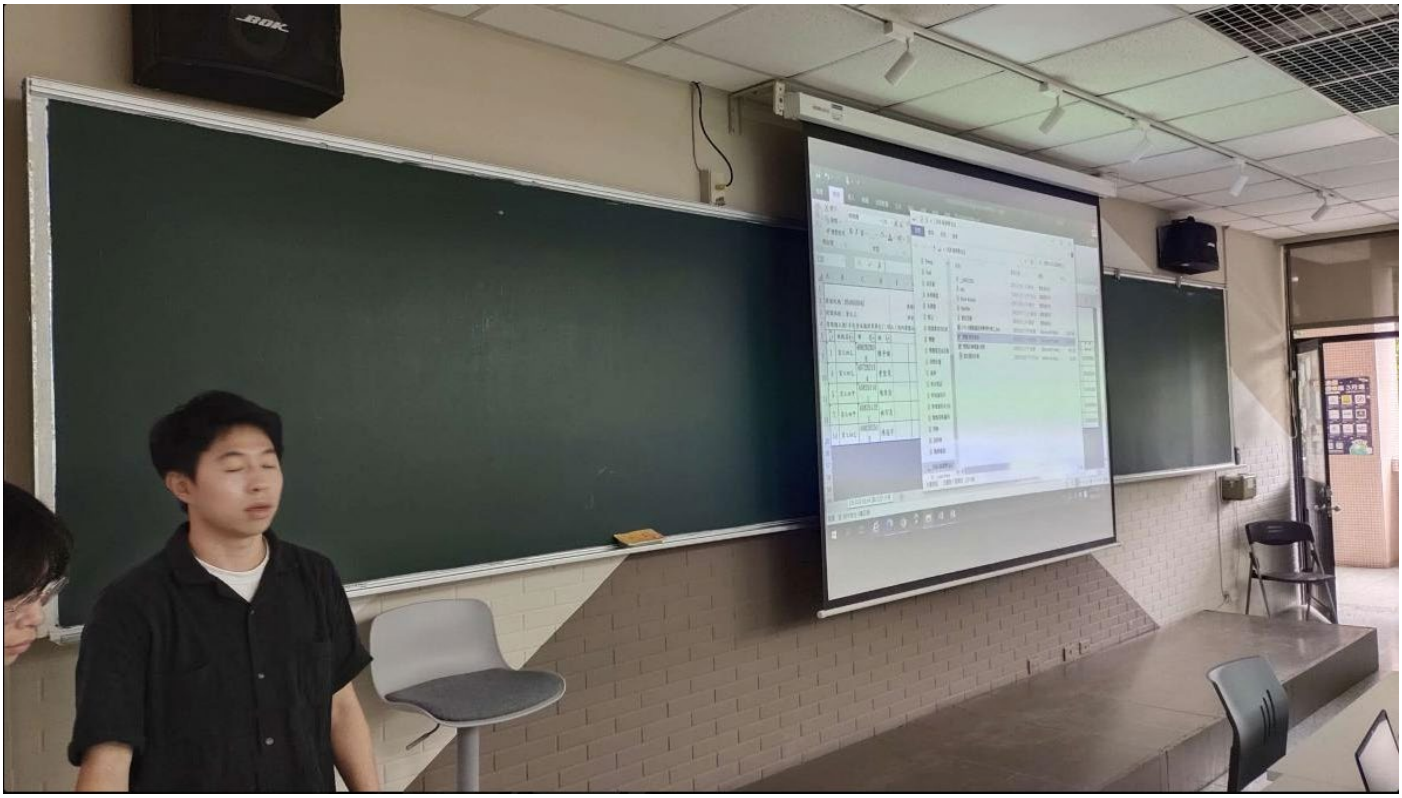
**三、學習心得(組內每位學生皆須提供至少 200 字的學習心得)**

老師上課講了許多，雲端計算的架構和技術，這篇論文則實際把邊緣運算運用在導航上，，讓用路人可以更快從導航上，收到最佳路徑，跟生活習習相關，能夠學以致用，但是還是偏向理論的部分，若是能使用軟體時做可能會更體會運端計算的功用。

**四、其它附件(必要)**

(一)每組學生成果 PPT

(二)分組討論及相關活動照片



# 2.7.1 課程指導紀錄表

學習助教：蔡濡謙

| | | | |
|---|---|---|---|
| 時間 | 2023/5/31 | 受指導組別 | 第七組 |
| 地點 | SF233 | 受指導次數 | 第___1___次 |
| 受指導對象 | **曹聖茂、陳冠宇** | | |
| 指導老師 | **林振緯 教授** | | |
| 指導內容摘要 | | | |
| 主要問題 | 參考論文報告蠻透徹的，但因為沒有實作，也可能是因為題目對設備需求比較大，如果可以模擬出一個環境展現出其差異，也是一個不錯的體驗。 | | |
| 具體建議與解決方案 | 類似論文的模擬問題與後續報告補充。 | | |
| 後續追蹤 | 後續實作相關的報告補充。 | | |
| 備註 | **無** | | |

*指導紀錄表請自行影印使用

**指導老師：_____林振緯_____**

附件二
每組填寫

# 輔仁大學 111 年高教深耕計畫【課程重構融入自主學習課程補助計畫】
# 學生自主學習計畫書

一、自主學習計畫主題：雲端技術在國軍數位學習系統上之應用

二、組別：第七組

三、課程名稱：雲端計算概論

四、指導老師：林振緯 老師

五、學生姓名與工作分配：(可以個人或團體方式執行，至多 5 人)

| 姓名 | 工作內容 |
|---|---|
| 曹聖茂 | PPT + 報告 |
| 陳冠宇 | PPT |
| | |
| | |

六、計畫內容與進度規劃 (請描述透過何種行動或方法達成)

先自行閱讀論文，然後透過跟組員的溝通、訊息交換得到更深入的了解，最後將訊息統整，上台報告。

七、預期效益：

預期將論文內容盡量完整的呈現

# 2.7.3 學生自主學習成果報告

撰寫日期： 112 年 6 月 14 日

**一、課程基本資料**

(一)自主學習計畫主題：雲端技術在國軍數位學習系統上之應用

(二)組別：第七組

(三)學生姓名：曹聖茂、陳冠宇

(四)課程名稱：雲端計算概論

(五)指導老師：林振緯 教授

**二、計畫成果**

(一) 自主學習歷程：（請回顧整個自主學習之執行步驟，摘要寫出歷程）

1.如何訂定主題？

在”臺灣博碩士論文知識加值系統”上尋找適合的主題

2.分工分配及執行狀況？

因論文內容稍多，於是跟組員分配章節，各自完成 PPT 並整合

3.是否遇到什麼難題？

閱讀論文時遇到一些陌生的名詞需要再上網查詢

(二)成效說明與實際產出：（可附加佐證資料、文書記錄、照片或相關計畫運作情形資料等）

附件附上 ppt

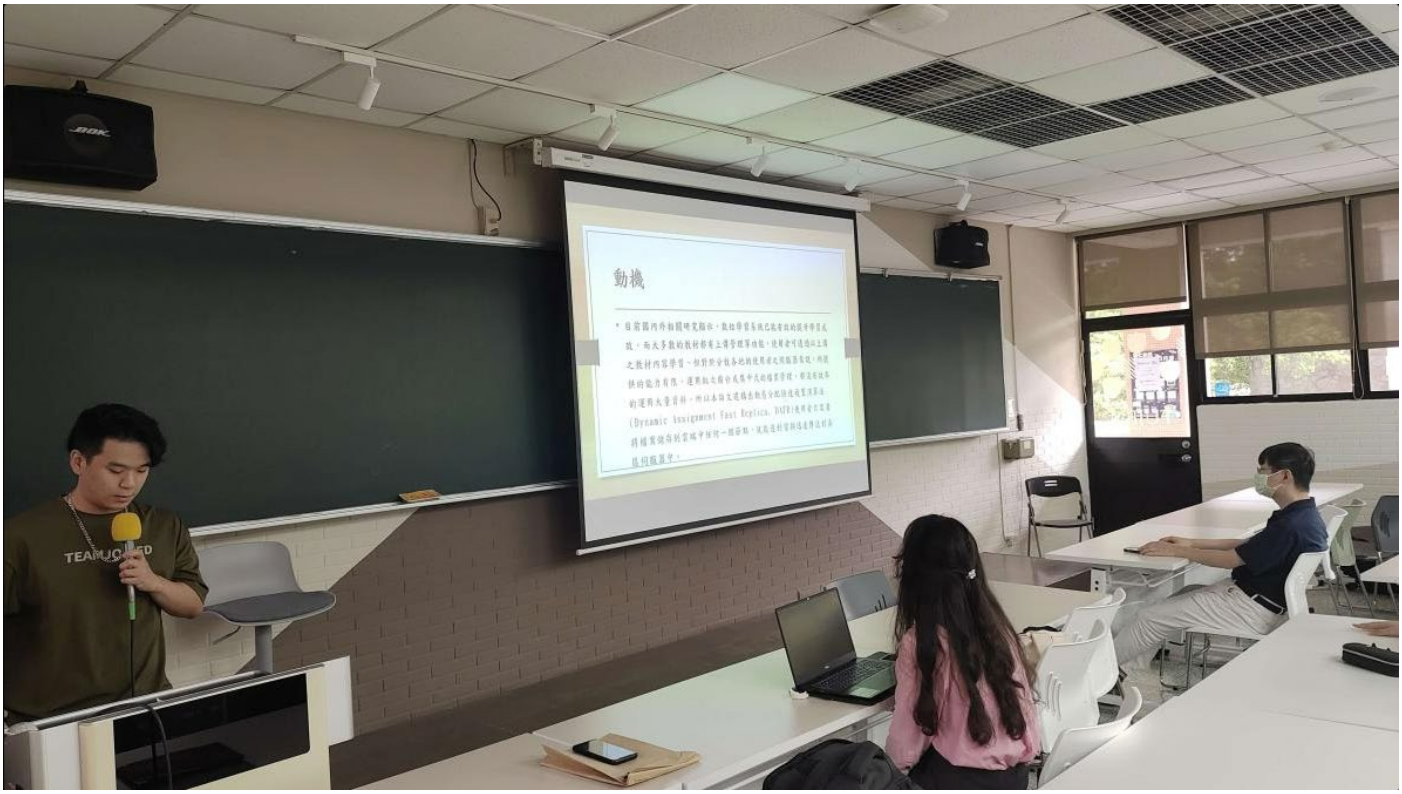
**三、學習心得(組內每位學生皆須提供至少 200 字的學習心得)**

**我認為這次的學習過程是很難得的經驗，從仔細挑選主題、更換主題、閱讀後遇到瓶頸需要尋找更多資料、跟組員交換資訊、整合資訊，考驗組員溝通能力及資訊整合能力，整體來說是獲益良多的一次學習。**

**四、其它附件(必要)**

(一)每組學生成果 PPT

(二)分組討論及相關活動照片



# 3. 優秀自主學習組別

## 3.1 組別 1 (第四組)

完整實作出兩種算法對於資源競爭的最佳化問題，雖然以雲端計算來說，演算法研究已經有點過於細節，跟雲端計算的架構部分相比差距甚遠。但藉由實作出兩種演算法來解決邊緣伺服器的資源競爭和分配問題，對於本課程的研究與實作達成部分的學習是一種重要的實作經驗，也是一個優秀的研究探討，可惜的部分是論文相關的結論與算法差異等等沒有展現出來。

## 3.2 組別 2 (第五組)

介紹了微服務架構並且嘗試模擬出來，雖然因為設備限制只成功做出部份實作，但其實要模擬出來的規模本來就不小，難度不小。後續也是完整了報告傳統的單體式架構與微服務架構性能上的區別，甚麼時候傳統的單體式架構會優於微服務架構，甚麼時候較新的微服務架構會比單體式架構性能更優秀，也做了不同的程式的運行比較，從此可看出挑選的論文質量也不錯。

## 3.3 組別 3 (第七組)

介紹了數位學習系統的雲端系統管理，對論文提供的方法介紹很詳盡，運用了動態分配快速複製演算法來將檔案快速上傳並發送至各個區域的伺服器中，論文也是提供了詳細的步驟介紹，整體報告流程也很順暢。

# 3.1 講座 1

講者: 胡家樺

演講時間: 2023.3.8 (三)

演講主題: 淺談資訊安全

資安（資訊安全）是指保護資訊免受未經授權的存取、使用、揭露、修改、破壞或干擾的一系列措施和實踐。隨著數位化時代的到來，資訊安全變得越來越重要，因為許多組織和個人都依賴於資訊系統和數位資產的安全運作。

資安的目標是確保資訊的機密性（保護資訊不被未經授權的人或實體所存取）、完整性（確保資訊在傳輸和儲存過程中不被未經授權的修改或破壞）和可用性（確保資訊系統和資源在需要時可正常使用）。為實現這些目標，資安採取了多種技術和措施。

講師這次演講特別親民，利用現今發生的一些國際規模的大型資安事件，例如中國駭客組織為竊取 5G 機密鎖定全球電信業者，北韓、中國等國家的資安攻擊，台灣的人民個資洩漏等等，業界的資安防護、還有日常常見的資安問題與一些預防的手段，像是帳號的密碼定期更換、帳號個資使用假資料等等，介紹一些日常常見的問題的解決方式，還有新型的資安攻擊方式的大概介紹。

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 游雅晴 |
| 業師名稱 | 胡家樺　講師 | 學號 | 408261357 |
| 時　　間 | 112　年　3　月　8　日 ( 三 )　AM 09:00-PM 12:00 | | |
| 學生心得 | 講師的工作經驗豐富，也跟我們介紹了很多資訊安全的相關工作，例如資安長，過去資安方面比較少受到重視，但隨著科技的發展，一些個資隱患也逐漸浮現，導致資訊安全越來越受到重視，甚至許多公司高薪聘請資安長，證明了資安是未來科技發展的重要問題。<br>資安事件層出不窮，講師有提到北韓、中國等國家都曾發生重大資安事件，例如中國駭客組織為竊取5G機密，鎖定全球電信業者，這些重大資安事件看似離我們遙遠，但其實我們身邊就有許多資安隱患，現在要竊取個資非常容易，我們很可能在無意間就洩漏了個資，而且防不勝防。<br>講師也跟我們介紹了幾種資訊安全常見的威脅，不僅有傳統的病毒攻擊，現在也有很多新的攻擊方式，因此資安防護措施也必須與時俱進，我覺得資安更重要的是提前防護，但這點還是比較難做到，是我們應該努力的方向。<br>最後講師還給我們看了一個有關ChatGPT的影片，其實ChatGPT的話題已經有一段時間了，但我還沒有很了解ChatGPT的詳細內容，看了影片後才比較了解ChatGPT的背景跟用處，之前在網路上一直看到一些言論說，ChatGPT會讓工程師失業，但看完影片後，我覺得ChatGPT更像一個工具，只要掌握工具的使用方法，就不需要害怕會失去競爭力，我還是比較認同”科技始終來自於人性”這句話，比起害怕被工具取代，倒不如把握學習的機會，讓自己變得更有競爭力。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 黃昱樵 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409261689 |
| 時　　間 | 112　年　3　月　8　日 ( 三 )　AM 09:00-PM 12:00 | | |
| 學生心得 | 這堂演講讓我了解了資安的重要性，首先講師分享了幾個事件，讓我意識到資訊方面的程式攻擊在現今社會發生頻繁，如果大企業遇到了網路攻擊勢必會造成，大規模的經濟損失，所以資安這方面的工作就變得更加重要，講師也講解了資訊安全有五個要點，機密性、完整性、可歸責性、可用性、可靠性。<br>後面講師講了資訊安全的認知，講了一些關於我之前都不知道的錯誤資安觀念，像是防火牆如果越多就越安全，這我之前都不知道這是錯誤的，後面介紹了幾種常見的病毒，有圖像是垃圾郵件、垃圾郵件、木馬、病毒、蠕蟲、間諜程式。其中像我自己有遇到過的圖像式垃圾郵件，現在知道了更多種的病毒類型。<br>最後我聽完了這次演講我覺得最有收穫的是講師教了我們資訊安全的防護措施，第一個是使用安全的密碼，定期更改密碼，密碼絕對不能用跟主機相關、生日身分證。還有一些推薦的密碼設定方式，再來是不隨便使用來路不明的程式，<br>要注意在網路上瀏覽資訊，COOKIE要記得刪除，要記得使用防毒軟體，定期更新。<br>這堂課讓我學到了更多我以前不知道的資訊安全知識。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 林紫琳 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409262243 |
| 時　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 聽完資安演講，我了解到國內外的資安事故，像是前幾年發生的裴洛西訪台的駭客攻擊，也學到一些日常的防護措施，在平常生活中要如何讓自己的個資、帳號更安全，還有一些設定密碼的小技巧。除了要定期更改密碼之外，更不要隨便連接來路不明的免費網路，是常見的網路釣魚手法；cookie紀錄重要的個人資料與網路使用習慣，也應隨手刪除電腦裡的cookie紀錄。<br>另外還了解到資訊長這個職務還有相關單位的責任以及證照，除了薪資優渥外，還要了解公司的IT的整體架構、洞悉可能的弱點，更重要的是具備跨部門溝通協調以及向上管理的能力，讓公司高層能認同管理措施。<br>並且符合以下條件:<br><br>1.必須成為足以在資深管理團隊發揮作用，且能夠與廣泛的技術與非技術人員溝通安全相關概念，是一位智慧型、辯才無礙又具說服力的領導者。<br><br>2.具備營運永續性規畫、稽核與風險管理，以及合約制訂與廠商協調的經驗。<br><br>3.必須對相關法令與執法單位圈具深厚的相關知識。<br><br>4.必須對資訊技術與資訊安全有紮實的理解。<br><br>讓我對資訊安全方面的工作內容感到興趣，但同時也覺得其壓力很大。<br>以下是我覺得很重要的筆記:<br>資訊安全 (Information Security)包含了：<br>Confidentiality：資料不得被未經授權之個人、實體或程序所取得或揭露的特性。<br>Integrity：對資產之精確與完整安全保證的特性。<br>Accountability：確保實體之行為可唯一追溯到該實體的特性。<br>Availability：已授權實體在需要時可存取與使用之特性。<br>Reliability：始終如一預期之行為與結果的特性。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 莊緗柔 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409261342 |
| 時　　間 | 112　年　3　月　8　日（三）　AM 09:00-PM 12:00 | | |
| 學生心得 | 科技發展的時代除了軟體技術趨於成熟外，資訊安全更是值得注意的一塊資訊領域，聽完演講後發現自己對於資安領域的不熟悉，案件數量遠超過自己的想像，買賣個資以賺取利益等事件層出不窮，或是因為政治立場的不同也會有許多在資訊安全上的攻擊，如2022八月裴洛西訪台時廣告刊版、官網、學校網頁等等都被植入反裴洛西的文字，因此基本的資安常識以及防範更顯得重要，分為機密性、完整性、可歸責性、可用性、以及可靠性，分別是對個人資料的授權與保密、資產完整安全保證、確保實體行為可追朔、授權實體在需要時可存取使用、以及始終如一預期之行為與結果的特性。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 陳冠宇 |
| 業師名稱 | 胡家樺　講師 | 學號 | 408262519 |
| 時　　間 | 112　年　3　月　8　日（三）　AM 09:00-PM 12:00 | | |
| 學生心得 | 這次的演講介紹很多資安相關的東西，也因為現在的時代，資安的重要性已經不能跟小時候帳號被盜的這種事件同日而語，事情小則一些相連的帳號無法使用，需要官方幫忙，大則某網銀的錢瞬間被掏空，上課中介紹很多攻擊的方式，跟為什麼，也介紹很多預防的方式:1不設帳號跟密碼相同或是簡單的英文、數字組合 2.密碼不要留在文字檔中 3.密碼越長越好解不要有明顯含意 4.不要用來路不明的網站 5.經常做防毒軟體的更新程式 6.防火牆要安裝　7 .cocokie 盡量要刪除 8.不要把帳號密碼在公共存取 ....等。<br><br>第二個重點是「chatGPT」這個軟體最近也很紅，很多網紅都有嘗試過使用、介紹，這次老師在上課放的影片也很有趣，除了讓我對此網站有很大的興趣之外，也很好奇如何達到這麼驚人的成果，從很久之前的圍棋AI就有這個疑問到現在，不過影片上也有說到，他們會故意或不小心錯一些很基本的小細節，我覺得可能是在模仿人類，但他錯的東西又比較不像一般人會犯錯的東西，這點我相信經過廣大人群一起訓練的情況下，會日益精進模仿的樣子，我還覺得設計著程式的團隊，除了有很強的技術能力以外，在對於行銷策略的那環也是很有一套，這東西需要很巨量的訓練，那開放給全部的使用者免費、付費使用，就是讓他直接跟現在的人類訓練，進而降低尋找新資料的困難及成本，總體來說很喜歡這次老師排的演講，在讀書之餘多了解一下最新的時事和提醒自己在網路上使用個人資料時必須小心的面向，很有收穫　。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 陳品璇 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409261110 |
| 時　　間 | 112　年　3　月　8　日（三）　AM 09:00-PM 12:00 | | |
| 學生心得 | 在這個網路資訊氾濫的時代，放在網路上的資訊都有可能被大眾所竊取盜用，而這些資訊對於企業、組織或個人而言，具有相當的影響力及價值是需要被保護的，於是有了大眾對於資訊安全的認知重視，而透過今天的講座，我對資訊安全的知識有了更深一層的啟發與了解。<br><br>講座的開頭，介紹了多起國內外重大資安事故，竊取機密、駭客攻擊、惡意攻擊程式、各種資安漏洞等，其損失重大且影響力遍及全球，讓人明確了解到其資訊安全不可忽略的重要性，以及嚴查防範的必要。<br><br>對於資訊安全之基本認識，其特性有，保護資訊之機密性、完整性、可歸責性、可用性、可靠性等，講者也介紹了幾種常見的病毒威脅，像是圖像式垃圾郵件、木馬、病毒、蠕蟲、間諜程式等，接著是入侵攻擊類，像是釣魚網站、分散式拒絕服務攻擊，搜尋引擎入侵、SQL指令植入式攻擊等，以及網路架設類，連線劫持、中間人攻擊，還有系統弱點類、無線網路攻擊類等，都是常用的手法。<br><br>光是這樣一聽,都覺得實在防不勝防,於是我認為透過平時的小動作來防範,降低駭客入侵，才是目前對於個人比較可行的意識認知，例如，定期更改更新密碼，並把握安全密碼的原則，在密碼設定時，將複雜係數提高，將滴被破解的可能，然後不要使用來路不明的程式，也是很重要的觀念，我認為這算是一種危機意識的培養，不要輕易將資訊洩漏的原則，還有防毒軟體、防火牆、cookie、隱私權、公用存取、網路詐騙、無限上網、備份等，都是平時能更加小心注意的地方。<br><br>我認為這場講座帶來很不錯的認知與體驗,雖說大家平時都強調資安的重要性，但卻缺少一個完整的管道，這場講座將資安的相關的知識，完整的講解，讓我對資安有更深一層的認識。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 林炫宇 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409262281 |
| 時　　間 | 112　年　3　月　8　日（三）　AM 09:00-PM 12:00 | | |
| 學生心得 | 我覺得胡教授的演講讓我受益良多，一步一步地帶著我們走入資安的世界。之前我對於資安都只是處於很片面的認識，只知道資訊安全這個名詞，沒想到其中有那麼多的奧秘。剛好這學期有修網路安全，和這一步部分有做連結，也讓我更熟悉資安。最後胡教授還有講到最近很紅的ChatGPT。經過教授播放的影片，我也更加地認識了ChatGPT。知道了它對我們的影響，以及我們要怎麼更好的利用它。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 吳家萱 |
| 業師名稱 | 胡家樺　碩士 | 學號 | 409262449 |
| 時　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 一、資安為甚麼重要<br>資訊安全人人有責，但不是人人等責，會依據你的工作性質和行為責任判斷你所需負的責任大小，而資安危機潛在於日常生活之中。<br><br>二、資訊安全基本概念<br>白帽駭客：好的駭客，通常是政府人員或資安企業的攻擊手/防護員，在經過你的同意後為你進行防護，透過漏洞測試的方式攻擊你的電腦(滲透測試)但會整理防護準則後為你進行防護，目的是協助防護你的電腦。<br>黑帽駭客：真的駭客，目的是要利用你的資料做對你有害的行為(例如:勒索)。<br>並不是防火牆越多層就越安全。<br><br>三、資訊安全的常見威脅<br>勒索攻擊：美國最大的石油公司收到勒索攻擊，導致當時油價高漲。<br>由於近年科技發展迅速，導致駭客日益變多，目前各大公司都會雇用資安長，因為是時代所需故薪資優渥。<br>連線劫持、中間人攻擊、無線網路攻擊(竊聽、通訊分析、偽裝、服務阻斷攻擊)、網路釣魚與網路詐騙。<br><br>四、資訊安全防護措施<br>使用安全的密碼、定期更改密碼、密碼設定原則、密碼不要留在紙上或文字檔中，不要太過信任公司、學校網路，不開放過多權限、備份/異地備份、零信任架構ZTA。<br><br>五、資安長介紹<br>想當資安長的話需要以下證照：CISA、CISM、CISSP、ISO27001LA。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 柯承佑 |
| 業師名稱 | 胡家樺　碩士 | 學號 | 409261055 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 最近，資訊安全議題成為了一個非常熱門的話題。身為一個資訊科技相關人員，必須要意識到資安對於個人和企業的重要性。在這場關於資訊安全的演講中，我學到了許多重要的事情。<br>首先，我們必須認識到資訊安全的威脅。現在有許多不同的方式可以破壞系統和盜取資訊。例如，這次的演講提到了很多駭客攻擊事件，更提到了國際資安人才的短缺，我們需要了解這些威脅，並學習如何保護自己。<br>我們必須熟悉各種資安工具和技術，以便更好地保護我們的系統和資訊。例如，防火牆、入侵偵測系統、加密技術和訪問控制等工具可以幫助我們保護我們的系統。同時，我們還應該學習如何使用這些工具和技術，以便更有效地保護我們的資訊。<br>我們必須保持資訊安全的意識。這意味著我們需要時刻關注安全問題，保持系統和應用程式的更新，使用更有安全性的密碼，限制訪問權限，以及定期備份重要資料等等。除此之外，我們還需要教育我們的使用者，讓他們了解如何保護自己的資訊，並提供資安相關的培訓。<br>總的來說，資訊安全是一個非常重要的議題。在這個數位時代，保護我們的資訊和系統變得更加重要。通過學習資安威脅、工具和技術，以及保持資安意識，我們可以更好地保護自己和企業的資訊安全。<br>在演講的最後講師有分享一些關於目前網路上蔚為話題的chatgpt的介紹飲片，裡面有許多議題是值得參考的，感謝講師能帶來精彩的演講，有助於提升我們的資安意識。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 邱晉寬 |
| 業師名稱 | 胡家樺　碩士 | 學號 | 409261079 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 講師向我們介紹薪資誘人並登上新聞的資安執行長,使人印象深刻外也分享了資訊安全的基礎知識。他解釋了資訊安全的重要性,並指出我們在日常生活中的數字足跡和數據交換都需要被保護。他還向我們介紹了資訊安全的三個核心原則,即機密性、完整性和可用性。通過學習這些基礎知識,我們可以更好地了解資訊安全的重要性和基本原理,並為未來的學習和職業發展打下基礎。<br>講師還向我們介紹了資訊安全領域的就業機會和挑戰。他指出,隨著數字化和信息化的發展,資訊安全行業正處於快速增長的階段,未來的就業前景非常看好。他還介紹了資訊安全領域的不同職業和職位,例如安全分析師、安全工程師、測試工程師等,以及相應的職位要求和技能要求。學生們可以通過學習相關的知識和技能,充分利用資訊安全領域的機會,實現自己的職業發展目標。<br>最後講師還介紹了一些實用的資訊安全工具和技術。例如,他介紹了一些用於保護網絡安全的防火墻和入侵檢測系統,以及用於檢測漏洞和弱點的漏洞掃描工具。學生們可以通過學習這些工具和技術,提高自己在資訊安全方面的技能,從而在就業市場上更具競爭力。<br>作為一名資工系的學生,我非常幸運地參加了這場精彩的資訊安全與就業演講。在這次演講中,講師向我們介紹了資訊安全領域的基礎知識、挑戰和機會,並分享了一些實用的工具和技術,讓我對資訊安全和就業方向有了更深入的認識和理解。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 林品瑄 |
| 業師名稱 | 胡家樺　講師 | 學號 | 408261668 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 關於這禮拜的演講，可以讓我們理解更多關於電腦防毒軟體的功能，也提到了防火牆，增加防火牆越多越安全，再來買珍貴的入侵偵測，就高枕無憂。Port口開越少就不會被入侵，交換過程中也不會被偷竊，如果沒有病毒，通知要把它關閉，就不會有任何危險。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 高楷昇 |
| 業師名稱 | 胡家樺　講師 | 學號 | 408261773 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 這場演講讓我更加了解資訊安全的重要性。在演講中提到，保障企業的資訊安全是非常重要的，因為一旦遭受駭客攻擊，不僅會造成企業的財務損失，還會影響企業的聲譽和客戶信任度。　在演講中，我學到了如何保障企業的資訊安全。例如：定期更新電腦系統和應用程式、使用強密碼、限制員工權限等等。同時也學到了如何預防和應對資安事件。例如：建立緊急應變計畫、<br>定期進行風險評估等等。<br><br>此外，在演講中我也學到了如何提升自己在資訊安全領域方面的技能和知識。例如：參加相關課程、閱讀相關書籍和文章、參加相關社群等等。 再者也更加認識到保障個人和企業的資訊安全已成為一個非常重要且必要的課題。同時也學到了如何保障自己和企業的資訊安全以及如何提升自己在資訊安全領域方面的技能和知識。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 朱永旭 |
| 業師名稱 | 胡家樺　講師 | 學號 | 408262375 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 聽完這場演講後，我體會到資安產業是一個不斷變化和創新的領域，並且隨著新技術的發展，資安產業也面臨著新的威脅和機會。還有臺灣資安產業也面臨著一些劣勢，像是市場規模小、法規制度不完善等。因此企業需要利用身份認證與零信任網路存取技術，自動化防禦系統等新技術來提升自身的防禦能力和效率。此外，也需要關注隱私保護法規以保護自身和客戶的安全。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 林家明 |
| 業師名稱 | 胡家樺　講師 | 學號 | 408262765 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 聽完胡講師的演講之後，我對於資安這方面認識到了更多，知道了一間公司來說，資訊安全是多麼的重要，例如對於金融公司，只要被盜取了資料，損失肯定難以估計，也了解目前市面上對於資安工程師非常缺少，國內外的薪水也都開得非常高，胡講師也對我們說了未來的發展方向，讓我更確定未來想要做的是什麼。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 陳新義 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409261108 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 這次聽了資訊安全的演講，學到了很多東西，像是資訊安全對於大大小小的公司(尤其是金融業)，非常重要，資訊安全保護資訊之機密性、完整性與可用性；得增加諸如鑑別性、可歸責性、不可否認性與可靠性。其中還包含很多方面，像是機密性，完整性，可靠性等等，現在在市面上，也有非常非常多種類的病毒，只要不小心點到不明的網址或是郵件就很容易中招，像是垃圾郵件，或是木馬程式，病毒，蠕蟲，或是間諜程式，有提到如何進攻以及如何防禦，分享了很多有關資訊安全的知識，最後也有讓我們看一個影片，是關於ChatGPT的影片，裡面講了很多有關的事情，邊跟觀眾分享有關的知識，邊用娛樂的講話方式讓影片不會無聊，同時也提到2040年人類將攻克絕症進入不死時代，利用最近很紅的ChatGPT還有AI的不斷學習，之後很多簡單的工作會被AI取代，可以剩下很多時間等等，總而言之，在這次的演講我學到了很多跟我科系相關的知識，也讓我比較知道之後學習的路可以怎麼走。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 王慧諦 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409261500 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 隨著科技的快速發展，資訊安全日益成為重要的議題。這次的演講中，聽到了許多因為資安引起的大小不一的資安事故，所以無論是個人或是企業，都需要注意自身的資訊安全，以免遭受到不必要的損失。透過這次演講，我深深體會到資訊安全的重要性，以下是我這次的心得。<br><br>首先，保護個人隱私是資訊安全的首要任務。在現今社會中，我們經常使用網路、手機等設備來進行各種資訊交流。然而，不當使用或不慎操作這些設備，可能會洩露個人隱私。因此，我們必須注意個人資料的保護，包括設置高強度密碼、不隨意填寫個人資訊、不下載未經認證的軟體等，以確保自己的隱私不被侵犯。<br><br>其次，企業也必須重視資訊安全。在企業運作中，資訊扮演著相當重要的角色，包括客戶資料、財務資訊、業務策略等等。如果這些資訊遭到竊取或損毀，將對企業造成巨大的損失。因此，企業需要建立完善的資安制度、定期更新防護措施，包括防火牆和系統，訓練員工的安全意識，像是不隨意開啟陌生郵件及保管好帳號密碼，以保障企業的資訊安全。<br><br>最後，保持學習和研究的心態，是資訊安全的基礎。資訊技術日新月異，資訊安全也需要不斷進步和更新。我們需要持續學習和研究，掌握最新的資訊安全技術和知識，並及時調整自己的安全策略。另外，也需要了解駭客最新的攻擊手段和技術，以便能夠更好地預防和應對攻擊事件。<br><br>綜上所述，資訊安全是一個持續不斷的過程，需要我們不斷學習及研究。只有重視資訊安全，並掌握好相關知識和技能，才能保證自己的重要資料不會輕易落入壞人手中。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 張庭豪 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409261641 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 今天的講座，讓我對未來多了一個方向，資安人員對每一個公司都特別重要，取代性較低，但要能夠勝任也需要一些挑戰，需要考一些相關證照，並對設計程式有一定的理解，才能防止有心人士攻擊你的電腦，這場講座中我學到，在資源爆炸的時代，隱私權對大眾來說特別重視，資安也越來越被重視，而我也有些興趣朝這個方向邁進，在大學時多累積一點實力，之後或許也能當上資安人員。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 許正吾 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409280489 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 這場演講很有趣，講者講得生動活潑，讓我對於資安問題和駭客攻擊有了更深入的了解。演講中，講者分享了各種最新的資安攻擊新聞，讓我更能夠了解現今資安問題的嚴重性。<br><br>講者提到，現在的網路世界中，駭客攻擊的手法越來越多樣化，如釣魚郵件、勒索軟體等等，這些攻擊不僅對企業單位造成傷害，一般民眾也面臨著被攻擊的風險。講者分享了一些實際的新聞案例，讓我更能夠理解資安攻擊的手法以及其危害性。<br><br>胡老師也分享了一些關於人生規劃的建議，我感到很有啟發性。老師提到，人生的路很長，我們需要學著如何自己去探索、學習新事物以及發現興趣所在和對事物的熱情，尤其是在我們 20-30 歲的時候。講者也鼓勵我們要勇於嘗試、不要害怕失敗，因為失敗是成功的一部分。<br><br>總而言之，這場演講讓我對於現今的資安問題有了更深入的了解，也學到了關於人生規劃的建議。講者的演講方式非常生動活潑，讓我很享受這次的學習體驗。我非常感謝講者的分享，也希望未來還有機會能夠參加類似的演講。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 曹聖茂 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409280489 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 這次演講主要著重在資訊安全，隨著科技的進步和互聯網的普及，資訊安全變得越來越重要。個人和企業需要注意保護自己的數據和隱私。資訊安全包括很多方面，例如防火牆、反病毒軟件、密碼學、加密和解密技術等等。<br><br>為了保護個人和企業的數據，我們需要學習如何管理和保護數據，建立安全的網絡環境，同時還需要意識到網絡安全的風險，例如身份盜竊、網絡釣魚、駭客攻擊等等。在這個不斷發展的領域中，持續學習和更新知識非常重要。最重要的是，每個人都需要認識到資訊安全的重要性，保護自己和他人的數據和隱私。<br>除此之外也對於資安長的工作有些許了解，雖然可能不是平常會接觸到的職業，但對於企業而言是不可或缺的存在。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 張嘉玲 |
| 業師名稱 | 胡家樺　講師 | 學號 | 407261659 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 聽完這次的演講，另我獲益良多。知道資訊安全對於我們生活中是很重要的東西，其實就跟我們生活習習相關。這次的演講老師講的非常的人讓人淺顯易懂，很令人會專注在老師所講的內容中。其中最有印象的就是演講快進入尾聲時播放的影片，其實人工智慧是一個工具不需要去懼怕，而是要學會如何去運用。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 邱柏翰 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409280312 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 這次演講提到了我經常聽到但基本上完全不了解的資訊安全,一方面資安在資工領域也算進階課程,另一方面我對其他方向更有興趣,目前還沒研究到資安的部分,所以能透過這次演講切入這個主題也是非常不錯。<br><br>現在駭客攻擊的方式已經越來越防不勝防了,尤其現在網路資訊發達,很多資工相關的code我都是在網路上學習的,那學習當然是先把程式載下來執行,如果裡面有惡意攻擊我大概也看不出來,但不執行我又看不到程式怎麼動的,所以也只能儘量使用高討論度社群的程式,和祈禱人們是善良的。<br><br>講師分享了很多在應用資訊軟體的時候應該注意的事情,但我覺得有點太多了,畢竟全部做到也不能保證100%安全,而且政府也會外洩資料,所以還是做一些基本的就好,不要亂點連結,不要亂下載東西,不要亂給權限,剩下就聽天命吧,該被駭還是防不住的。<br><br>總體來說,我在這堂演講認識到的資安,就像是法律一樣,彷彿有一本比六法全書還厚的資安注意事項,而且基本上每天都在更新,律師還只要在政府修法的時候看看新條文,但資安工程師看新文件好像是日常任務,讓我感覺資安這條路不太適合我,太過於瑣碎了,感覺就是每天追著新漏洞跑,和世界上任何一個角落的駭客進行一場永遠不會結束的戰爭。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 林俞駿 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409262396 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 聽過今天的這場演講之後，讓我感覺對資訊安全又有更進一步的了解，最近幾年來，網路發展得十分迅速，電腦越來越普及，幾乎每個人都需要上網，這也更突顯學習”資訊安全”是非常重要的，演講中胡老師提到駭客可能會如何竊取他們想要的資料，所以我們應該如何預防，還提到除了駭客本人外我們可能還需要堤防身邊的親戚好友，因為如果親戚好友比較沒有資訊安全相關知識的話，在群組間轉傳的鏈結說不定就是有問題的鏈結，我覺得這是非常受用的，因為這是最貼近我們生活，最有可能會遇到的事情。這次的演講真的很實用，不管事在自己平常生活上網時如何保護自己，還是未來出社會時，如果學習這項技能會有什麼幫助，湖老師都講得十分具體。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 陳祈叡 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409261548 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 在本次兩個多小時的演講中，提到了許多有關資訊安全方面的知識。包含從一些新聞案例中了解到資訊安全的重要性，和當中資安事故所造成的嚴重影響，以及我們平常可能會遇到的資安攻擊與應做防護措施等等。後面甚至還有提到一些業界相關內容，如資安人員的職責、資安相關證照考試，甚至是與講師專業領域相關，保險方面中一些資訊相關法規等等，使我對於資安領域在業界中的結合應用有更進一步的了解。<br><br>除了學到更多資訊安全的知識外，在一開始老師介紹講師時，提到講師任教於銘傳大學風保系，甚至後來講師在自我介紹時也有提到自己先念了應用數學系後又念了法律研究所，讓我思考了一下這些跟資訊安全的關聯。不過在後來講師介紹到自己的工作經驗，以及聽完演講內容後，讓我領悟到，這其實也算是多領域結合吧，也讓我很敬佩講師有多方面的專業才能與工作經驗，精神相當值得學習。本次的演講可說是內容豐富，令我收穫滿滿。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 李維琪 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409261627 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 今天的課程林教授邀請了胡家樺老師來跟大家分享資訊安全相關的資訊,胡老師從介紹資安為何重要為起頭,開始分享國內外曾經發生過的資安事件,來讓我們迅速的進入狀況,感受到資安危機的嚴重性。其中最讓我印象深刻的就是因為各類的資安事故,進而變得更加被大眾重視的職業:資安長,資安長必須兼備管理領導和技術能力,他需要與管理階層合作,作為技術層和管理層之間的橋樑,在企業被駭客攻擊之時,也要能當機立斷的做出判斷,所以是一種薪水很高,但責任也相對很重的職業。<br><br>在解釋何謂資安之後,老師也介紹了很多種的資安攻擊方式,我認為在生活中最有機會遇到的就是無線網路攻擊。以前還未申請手機網路方案前,我很常點開WIFI功能,尋找著免費的網路來連線,通常在第一次連線的網路,手機都會跳出是否信任這個網路來源的選項,以前的我都會毫不猶豫地按下信任,但現在我知道這是非常危險的行為,無線網路藉由開放的空中電波,幾乎無法控制其實體存取,所以可以輕鬆地竊取資料,讓你連資料什麼時候外洩的都不知道,是現今網路世代非常需要注重的資安問題。胡老師提供了不少防護資訊安全的措施來給大家參考,讓我們有更多的選項來幫助自己保護自身的資訊安全。<br><br>在演講的尾聲,老師介紹了如果想從事資安方面的工作,大家可以去考哪類的相關證照、接受什麼樣的課程訓練來讓自己精進資安的能力,最後也分享了近期造成轟動的chatGPT,來讓我們對人工智慧有些初步的認識。胡老師的經歷豐富,也在各領域中都有所涉略,講解的內容詳細、富有專業性,給了大家不少未來求職相關的建議與方向,讓我們此次的演講活動受益良多。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 林家賢 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409261574 |
| 時　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 一聽到胡老師的演講，就可以深深感受到老師對資訊產業的熱情，這場演講一共有 5 個重點，分別是資訊安全為什麼、資訊安全基本概念、資訊安全的常見威脅、資訊安全防護措施和資訊長及資安專責單位，首先，由於現代社會越來越依賴資訊科技，越來越多的人和組織（公司、銀行、政府等）都使用數字資訊來處理敏感和重要的資料，近年來有不少重大的資安事件都導致很多人的利益受到損害，像是鎖定蘋果 M1 處理器的惡意程式 GoSearch22，中國駭客組織竊取 5G 機密或是北韓駭客組織發起的社交工程攻擊，這三件都是讓我們重新省視自己平常對於個人資安保護是否不夠妥當，這些所謂的駭客經常透過網路的漏洞或是一些釣魚軟體，用一些容易誘惑人的言語，讓一些貪小便宜的人上當，因而獲取個資進而獲取更多利益，再來，資訊安全是什麼呢？ 部分資訊是可透過網路來互通共享的，但部份資訊是屬於不可公開且不可篡改的，必須作保密的管制以防使用者有意或無意的讀取或更改，有關資訊保護之研究的總合就稱為資訊安全。這些資訊對企業或組織而言都是有價的，對企業或組織的營運有相當的影響。因此，需要賦予適當的保護，降低其風險，避免遭受內在或外來的威脅。不過即使裝了防火牆、防毒軟體，或是各種防禦工具，還是沒有 100%完全防禦，因為駭客總會試著跳過各種防禦系統找出新的方法，入侵你的系統，維護資訊安全不只是你我的責任，更是每個人的責任，我們應該要連有經過認證的無線網路，因為傳統的有線網路要竊取傳輸資料，必需去連接實體線路或設備才能監聽，而無線網路卻只要經開放的空中電波，幾乎無法控制其實體存取，輕易地就可以竊取傳輸資 料，造成許多無線網路的攻擊，而關於密碼的設定，也有一些安全規則可循，密碼越長越好，最短應該在八個字以上，密碼不要有明顯含義，最重要的是密碼要能記得住，一個連自己都記不住的密碼是無意義的，一個不易被破解的密碼應至少有一個英文大小寫、一個數字、一個特殊符號且沒有任何意義的組成。cookie 紀錄重要的個人資料與網路使用習慣，應隨手刪除電腦裡的 cookie 紀錄。<br>最後，因應資訊安全的潮流，各大組織及企業紛紛設立自己的資安單位，維護自己和客戶的權利，然而監督與協調整體企業安全任務的人就是資安長，在薪資上可說是相當優渥，但成為資安長的條件也相當嚴苛，需要在資深管理團隊裡發揮作用，能夠與所有人溝通安全相關概念，具備合約制訂與廠商協調的經驗，必須對相關法令與執法單位具深厚的相關知識以及對資訊技術與資訊安全有紮實的理解。這場演講讓我不只了解什麼是資訊安全以及個人資料的保護，也讓我看到另一條未來工作可能發展的方向。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | 淺談資訊安全 | 學生姓名 | 吳奕楨 |
| 業師名稱 | 胡家樺　講師 | 學號 | 409262308 |
| 時　　間 | 112 年 3 月 8 日 ( 三 ) AM 09:00-PM 12:00 | | |
| 學生心得 | 一、 資訊安全為什麼重要?<br>資安的重要性在現代社會日益增加，因為越來越多的業務和個人資訊都存儲在數字化形式中，並通過網絡傳輸。以下是幾個關於資安重要性的原因：防止數據損失和經濟損失：未受保護的系統和數據易受到駭客攻擊、病毒感染和其他安全漏洞的影響。這可能導致數據丟失、損壞或被盜取，進而導致業務損失和經濟損失。<br><br>保護個人隱私：個人資料可能包括信用卡號碼、銀行帳戶信息、健康記錄等敏感信息，如果這些信息遭到未經授權的訪問，可能會對個人造成嚴重的損害和影響，包括財務損失、信用評分下降和身份盜竊等。<br><br>維護企業聲譽：一旦企業系統遭到駭客攻擊或敏感信息外泄，可能會對企業聲譽造成長期影響，客戶可能會失去對企業的信任，進而影響業務的發展和獲利。<br><br>遵守法規和條例：隨著數據隱私和安全問題日益嚴重，許多國家和地區制定了相應的法規和條例來保護數據安全和隱私。企業和個人必須遵守這些法規和條例，否則可能會面臨罰款或法律責任。 | | |

| | |
|---|---|
| 學生心得 | 二、資訊安全基本概念<br>是指保護電腦系統、網路、應用程式和數據不受非法訪問、損壞或泄漏的能力。以下分為幾種特性：<br><br>機密性：資料不得被未經授權之個人、實體或程序所取得或揭露的特性。<br>完整性：對資產之精確與完整安全保證的特性。<br>可歸責性：確保實體之行為可唯一追溯到該實體的特性。<br>鑑別性：確保一主體或資源之識別就是其所聲明者的特性。<br>不可否認性：對一已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。<br>可用性：已授權實體在需要時可存取與使用之特性。<br>可靠性：始終如一預期之行為與結果的特性。<br>三、資訊安全的常見威脅<br>病毒類：<br>垃圾郵件：是未經收件者同意，即大量散發的郵件，信件內容多半以促銷商品為意圖，是某些想利用網路致富的人，藉以散播廣告或色情的媒介。<br>木馬：是一種惡性程式，和病毒最大的不同是，特洛伊木馬通常不會自我複製，大多用來竊取電腦密碼，它只是一種遠端管理工具，而且本身不帶傷害性，也沒有感染力，所以不能稱之為病毒，這種程式主要目的就是窺視每台電腦中的機密，例如信用卡卡號、身分證字號、銀行帳號、各式帳號密碼等。<br>入侵/攻擊類：搜尋引擎入侵：指的是利用搜尋引擎的進階搜尋字串，找到企業網站的關鍵資訊。目前 Google Hack 入侵手法得以成功，追根究底，原因往往出現在許多網頁程式寫法出現問題，可以利用搜尋引擎，找到網站設定檔外，也可以利用鍵入內部網址、或者是搜尋網站目錄、檔案類型等方式找到包含網站伺服器檔案、帳號、密碼、管理介面等資料，在交叉分析這些結果，能找出關於某個網站的資訊，甚至所揭露的資訊多到足以讓人入侵其網站伺服器。<br><br>網路釣魚：是企圖通過電子郵件或即時通訊訊息，把用戶誘騙至官方外觀幾無二致的假冒網站，冒充真正需要信息的值得信任的人，欺詐性地獲取敏感的個人信息（比如密碼和信用卡細節）的行為。它是社會工程攻擊的一種形式。<br><br>系統弱點類：DNS 快取記憶體下毒：直接攻擊網域名稱系統伺服器，一方面直接篡改 DNS 伺服器內容，一方面向其他 DNS 伺服器或網路上任何查詢請求，提供假造的 DNS 遞迴資訊服務。 |

網路架設類：連接劫持：連線劫持會欺騙伺服器或用戶端，把上游的主機當成實際合法的主機。上游的主機會由操控網路的攻擊者主機所取代，讓攻擊者的主機看起來像是所要的目的地，監視網路流量，如發現網路中出現大量的 ACK 包，則有可能已被進行了會話劫持攻擊。

中間人攻擊：發生在攻擊者攔截您和預期的收件者之間傳送的訊息，然後攻擊者會變更訊息並傳給原始的收件者，收件者收到訊息，看到訊息是來自您，然後就依照訊息指示動作，當收件者將訊息傳回覆您，攻擊者會中途攔截，並加以變動，然後再傳回給您，您和您的收件者永遠都不知道曾經被攻擊過。

無線網路攻擊：竊聽：竊聽是指入侵者針對無線網路通訊內容進行監控，利用竊聽內容來獲取被害人的個人資料如帳號／密碼等；最常見的例子是於無線網路登入時竊取被害人的登入帳號密碼。

訊息竄改：訊息竄改指攻擊者針對無線網路通訊的內容進行增刪或者更動。

四、資訊安全防護措施使用安全的密碼、定期更改密碼、密碼別留在紙上或是文字檔中、不要任意使用來路不明的程式、使用防毒軟體及定期更新病毒碼、應隨手刪除電腦裡的 cookie 紀錄、不任意在從未聽過，或第一次造訪的網站中，填寫重要的個人資料、絕不勾選網路瀏覽器的「記住密碼」選項、盡量不在公用電腦中輸入敏感性高的資訊、勿點選電子郵件上提供的超連結、啟動防毒軟體與防火牆，並更新到最新狀態。

五、資訊長及資安專責單位資安長將監督與協調整體企業安全任務，包括資訊技術、資源、通訊、法律、設備管理與相關部門，確保安全防護措施有效率及效果並制訂標準。必須成為足以在資深管理團隊發揮作用，且能夠與廣泛的技術與非技術人員溝通安全相關概念，是一位智慧型、辯才無礙又具說服力的領導者，同時具備營運永續性規畫、稽核與風險管理，以及合約制訂與廠商協調的經驗，也必須對相關法令與執法單位圈具深厚的相關知識、對資訊技術與資訊安全有紮實的理解。

# 3.2 講座 2

講者: 張致恩 博士

演講時間: 2023.4.26 (二)

演講主題: Introduction to differential privacy

差分隱私（Differential Privacy）是一種隱私保護技術，用途是在處理和發佈敏感性資料時保護個人隱私。差分隱私的目標是確保在對資料進行分析和查詢時，不會洩露關於特定個體的敏感資訊。

差分隱私通過在資料處理過程中引入噪音或擾動來保護個人隱私。這種噪音的引入是有控制的，以便平衡資料的準確性和隱私保護的需求。差分隱私技術可以應用於各種資料處理場景，包括資料聚合、機器學習和資料採擷等。

在差分隱私的框架下，資料處理者需要採取一系列隱私保護措施，以確保資料集中的個體資訊不會被洩露。這可能涉及添加噪音、對查詢結果進行修正或限制資料訪問等方法。

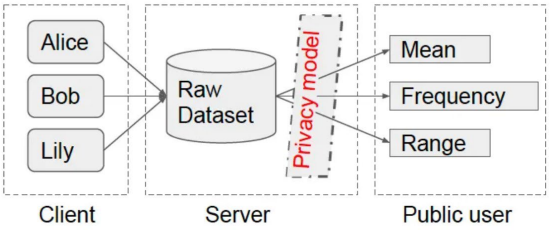
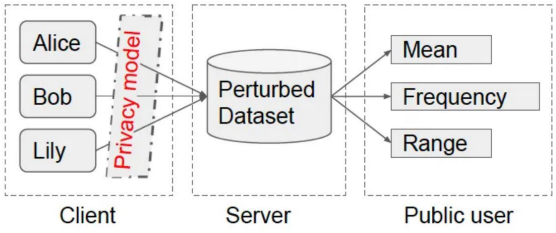
差分隱私提供了一種形式化的隱私保護模型，它可以量化資料隱私的保護級別，並提供數學理論和演算法來實現隱私保護。這種技術在隱私保護領域得到了廣泛應用，尤其是在處理大規模敏感性資料時，如醫療記錄、個人偏好和社交網路資料等。

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 王慧諦 |
| 業師名稱 | 張致恩 博士 | 學號 | 409261500 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 在數字化的時代，我們所產生的數據已經成為了一種資源，而這些資源的使用與共享也變得越來越普遍。然而，隨著數據使用和共享的不斷擴大，隱私保護的問題也越來越受到關注。對於個人隱私的保護已經成為了一個重要的問題。因此，在這種情況下，保護個人隱私的方法和技術也變得越發重要，其中包括privacy budget、privacy framework及Laplace mechanism等。<br><br>首先，在數據分析過程中，可能會出現敏感信息洩漏的問題。privacy budget就是在限制敏感信息洩漏的前提下，允許系統在數據分析過程中洩漏的敏感信息的最大數量。通過限制敏感信息的最大數量，可以有效地保護個人隱私，防止數據被濫用或遭受侵犯。在實際應用中，根據具體情況調整privacy budget的大小是非常重要的，以達到更好的隱私保護效果。<br><br>接著，在數據隱私保護中，常見的privacy framework包括differential privacy等。differential privacy是一種強大的隱私保護技術，它是通過在數據中添加一定的噪音來實現數據隱私保護。這項技術在保護個人隱私的同時，同時也保持了數據的可用性，因此得到了廣泛的應用。differential privacy通常包括三個主要元素：數據集、查詢和隱私預算。其中，隱私預算就是privacy budget的一個具體實現，它限制了查詢所能引起的隱私損失的最大量。因此，根據數據集和查詢的不同，可以通過調整隱私預算的大小來保護數據隱私。<br><br>最後，Laplace mechanism是一種常見的差分隱私技術，它通過向數據中添加一定的Laplace噪音來實現隱私保護。這種方法的優點在於它可以很好地保持數據的可用性，同時還可以實現較高的隱私保護強度。這種方法的缺點在於需要進行參數調整，且參數調整的不當會導致數據的實用性下降。因此，在實際應用中需要根據具體情況選擇合適的參數值，以達到最佳的隱私保護效果。<br>總之，privacy budget、privacy framework以及Laplace mechanism是現代數據隱私保護的重要技術和方法。隨著數據使用和共享的不斷擴大，隱私保護的問題也越來越受到關注。在選擇隱私保護技術和方法時，需要根據具體情況和需求進行選擇和調整，以達到最佳的隱私保護效果。同時，需要注意的是，數據隱私保護是一個不斷發展和演進的領域，我們需要不斷地學習和更新相關知識，以保持對這個領域的了解和掌握。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 林紫琳 |
| 業師名稱 | 張致恩 博士 | 學號 | 409262243 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | Differential Privacy<br><br>What is Differential Privacy?<br><br>大數據時代的數據爆炸導致個人（如個人）和實體（如組織、公司和政府）產生和持有大量數據，如個人圖像、財務記錄、醫療記錄、交易記錄 日誌和人口普查數據。同時，當數據離開數據所有者的手並參與某些應用程序時，會引發嚴重的隱私問題。<br><br>Tradeoff between Privacy and Utility<br><br>在數據發布中，已經設計了泛化和分桶等匿名技術來提供隱私保護。 同時，降低了數據的效用。重要的是要考慮隱私和效用之間的權衡。通過比較隱私增益和數據匿名化帶來的效用增益。<br><br>DP vs. LDP<br><br>1) Centralized Differential Privacy (DP)<br>Assumed that Data Curator can be trusted. (Data Curator collects data from individuals and publishes privacy-preserving statistics)<br><br>2) What if when individuals do not trust the data curator?<br>LDP: individuals send their data to the data aggregator after privatizing data by perturbation. These techniques provide plausible deniability for individuals. Then, The data aggregator collects all perturbed values and makes an estimation of statistics (e.g. frequency estimation).<br><br>Plausible deniability<br>Plausible deniability is the ability to deny any involvement in illegal or unethical activities, because there is no clear evidence to prove involvement.The lack of evidence makes the denial credible, or plausible.The use of the tactic implies forethought, such as intentionally setting up the conditions to plausibly avoid responsibility for one's future actions.The term is used both in law and in politics. In politics, plausible deniability usually applies to the practice of keeping the leadership of a large organization uninformed about illicit actions that the organization is carrying out. | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 林政宏 |
| 業師名稱 | 張致恩 博士 | 學號 | 409261093 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 我覺得今天的演講其實沒有演講的感覺, 比較像是上課的方式, 這次的講師說他目前在台大當客座教授, 之前在美國教書, 所以能體驗到不同的上課方式蠻開心的, 相較於在學校的課程, 撇除上課的內容, 感覺上多了一些的例子, 講師也很積極的想和大家互動, 所以這次的體驗還算不錯, 還有一點蠻有趣的,就是講師一直以為這一次來演講的班級跟上一次是一樣的, 所以有時候會問一些上次的問題. | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 陳品璇 |
| 業師名稱 | 張致恩 博士 | 學號 | 409261110 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 隨著互聯網技術和大數據的快速發展，數據隱私保護問題也越來越嚴峻。差分隱私是計算機科學和統計學中的一個概念，旨在在允許對敏感數據進行分析的同時保護個人隱私。也是因為這個原因，受到了人們的廣泛應用。講者也詳細的介紹有關差分隱私這一概念以及其在數據保護方面的應用。<br><br>關於差分隱私的基本概念，差分隱私是一種能夠保護數據隱私的技術，它在統計查詢或數據分析中添加噪聲，使攻擊者難以區分任意兩個個體的數據。也就是說，即使攻擊者能夠訪問數據分析的結果，也無法確定其中是否包含某一個特定個體的數據。而這種技術可以廣泛應用於各種場景，包括數據分析、機器學習和隱私保護系統的設計等領域。<br><br>從中我們能了解到差分隱私相比於其他數據隱私保護技術有什麼優勢呢？它能夠在保護數據隱私的同時，最大程度地保留數據的可用性，使得數據能夠得到更加精確的分析和應用。而且差分隱私具有很好的前瞻性和適應性，能夠根據數據的變化和不同場景的需求進行調整和優化。<br><br>講座也介紹了差分隱私在實際應用中的一些相關案例。差分隱私技術可以應用在醫療數據的分析，這對於醫學研究和治療方案的制定都有很大的意義。此外，在交通出行和智慧城市建設等領域，差分隱私也能夠發揮重要作用。例如，可以使用差分隱私技術對人群的出行情況進行分析，以更好地制定城市交通規劃。<br><br>最後我們應該更加關注數據隱私保護問題，並且應該在實際應用中積極探索和應用差分隱私技術，以更好地保護個人隱私和促進數據分析和應用的發展。我們需要更多的專家和學者深入研究和探討差分隱私技術的理論和應用，為推進數據安全和隱私保護作出貢獻。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 吳奕楨 |
| 業師名稱 | 張致恩 博士 | 學號 | 409262308 |
| 時　間 | 112　年　4　月　26　日　( 三 )　AM 09:00 – AM12:00 | | |
| 學生心得 | Random Noises in DP<br><br>1)　Too small : cannot provide enough protection<br><br>2)　Too large : aggregated data become meaningless<br><br>3)　Sensitivity : the largest possible different that the private information to make Laplace Mechanism : Laplace Distribution with scale b is defined by the probability density function as :<br><br>CDP v.s LDP　：<br><br>$$Pr[v] = \frac{1}{2b} e^{\frac{-\lvert v \rvert}{b}} \text{ where } b = \frac{\Delta f}{\epsilon}$$<br><br>  <br>(a) Centralized differential privacy<br><br>  <br>(b) Local differential privacy<br><br>CDP：<br>集中的資料管理員收集所有資料，然後在向公眾釋出之前使用DP進行擾動<br>LDP：<br>在使用者離開使用者裝置之前，在本地擾動使用者的資料，只有資料所有者才能訪問私人資料，資料管理員只持有擾動資料 缺點：與CDP相比，效用較低 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 吳家萱 |
| 業師名稱 | 張致恩 博士 | 學號 | 409262449 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 有關隱私洩漏、隱私預算、Laplace機制、機率密度函數、隨機回答和集中式差分隱私（DP）等主題的心得。<br><br>隱私洩漏是個人敏感信息在未經授權的情況下被揭示或公開。這可能導致身份盜竊、信用詐騙等嚴重後果。隱私預算可以被視為限制數據處理操作對個人隱私影響的上限。通過設置合理的隱私預算，我們可以控制數據處理操作中的洩漏風險，同時保護個人隱私。<br><br>Laplace機制是一種常見的隱私保護方法，這種機制通過在數據中引入噪音來保護個人隱私。Laplace機制使用拉普拉斯分佈的機率密度函數來生成噪音，並根據隱私預算的要求調整噪音的強度。這種方法在保護隱私的同時，仍然能夠提供有意義的統計結果，使得數據分析成為可能。機率密度函數在統計學和機率論中起著重要的作用。它描述了一個隨機變量在不同取值下的機率分佈。這個函數可以幫助我們理解和分析數據的特徵以及事件發生的機率。通過對機率密度函數的研究，我們可以更好地理解和應用機率統計的方法來處理問題。<br><br>隨機回答是一種用於保護個人隱私的技術。在某些情境下，人們可能不願意或不敢坦率地回答一些敏感問題，因為他們擔心自己的回答會被揭示出來。隨機回答通過引入隨機性來模糊真實的回答，從而保護個人隱私。<br><br>集中式差分隱私是一種隱私保護框架，旨在保護個人數據的隱私。它通過在數據處理過程中引入噪音來達到隱私保護的目的。與其他方法不同，集中式差分隱私將隱私保護的責任集中在數據處理中心，以確保數據的隱私性。這種方法可以在保護個人隱私的同時，提供有效的數據分析和共享。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 林佑宥 |
| 業師名稱 | 張致恩 博士 | 學號 | 409261251 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | Differential privacy是指利用資料差異來得知新增的差異資料內容而導致資料外洩。解決方式是使用random noise來加密修改原資料內容，假如兩份資料類似則無法分辨解讀出正確的差異內容。private budget(正常值介於0.001-1之間)是指隱私資料外流程度的容忍值，private budget越高代表外流資料越無所謂，代表random noise可以越小不去加密修改原本的資料。random noise的修改值要選擇適當的值，太大雖然保護越佳但也會讓資料失去原本意義，太小則會變成沒有加密顯現原本的資料。假如遇到資料是binary machanism要用random noise加密時可以用直硬幣的概念來實作，當中有p+(1-p)*p回答是0，(1-p)*(1-p)回答1，而當中只有p是正確的，(1-p)是有加密的。這個加密方法可以提供plausible deniability，讓每個人的資料都可以各自受到一定程度的保護，讓資料沒辦法能直接正確的對應每個人。最後在解密時就可以利用當初distribution 的分配狀態來反推出總體的大致接近正確資料的個數集合，但並非完全精準的個人個別資料。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 林炫宇 |
| 業師名稱 | 張致恩 博士 | 學號 | 409262281 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 我覺得這次演講讓我受益良多，因為這次所講的主題是我從來沒有接觸過的。<br>這次演講讓我知道了noise的功用及用法，資料加上noise之後既不會和原始資料相差太多，失去意義，並且還能夠對資料進行保護。<br><br>我還學習到了Plausible deniability這個特殊名詞。這句話直翻是似是而非的否認，一開始聽到這個詞覺得老師到底在講什麼，後來經過老師的解釋之後，便慢慢懂了。我很感謝張教授帶給我們如此精彩的演講，希望之後還有機會能夠再上張教授的課。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 邱柏翰 |
| 業師名稱 | 張致恩 博士 | 學號 | 409280312 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 這次演講講到了差分隱私，蠻有趣的，我沒想過統計資料也可以造成資安問題，原本保護原始資料就夠麻煩了，現在感覺資安真的很精深，也讓我有點畏懼，偶爾當演講聽聽感覺很有趣，但長期學習應該很快會感到無聊，尤其今天在教授投影片中看到久違的拉普拉斯函數，本校資工系對數學教學的部分我認為是偏弱的，這代表要踏入資安之前我可能得先學更多工程數學，所以還是算了，就當是知識科普就好，我應該不太適合這個方向。<br><br>尤其前陣子看RSA非對稱式金鑰加密的數學計算，看到有點煩躁也沒有非常了解，或許我對數學的興趣不及程式碼。<br><br>在演講的最後提到了合理推諉（plausible deniability），還蠻有趣的，指的是該事實與當事人之前並沒有絕對直接的關聯，所以當事人可以否認該事實。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 柯承佑 |
| 業師名稱 | 張致恩 博士 | 學號 | 409261055 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 這次的主題比較高深，主要是與加密有關。聽了這次的演講讓我知道一些以前就有的疑惑，在我們於網路上填寫資料時，有時候會擔心在傳輸過程中會不會被偷窺我們填寫的內容，尤其是當我們需要填些自己的基本資料時尤為擔憂。萬一途中被有心人士擷取，後果會非常麻煩。今天的演講中正好解答了我的疑惑，我在今天的課了解到了一些能有效保護客戶端傳遞資訊的機制，這種方法可以透過操作固定的機率來改寫客戶端原本填寫的資訊，例如我們填寫「是」，這個機制會使用一個公式來使部分回答更改為「否」，反之亦然。當傳輸到目的端時解碼回到原樣，整套流程下來效率很高且也能有效讓資料得到保護。在聽完今天的演講，對於這類資安方面的知識有了很大的提升，對於近年世界對於資安越來越重視的情況下，多了解這方面的是能帶給我們很多幫助，也讓我們資工科的學生更好將學到的知識聯繫上世界的變化，如果之後還有相關的演講我也樂意去聽已學到更多。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 曹聖茂 |
| 業師名稱 | 張致恩 博士 | 學號 | 407262134 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 感謝張教授分享有關differential privacy的內容，這場演講對我來說非常有價值，因為我從中學到了如何使用Differential Privacy保護個人隱私，同時仍然能夠應用分析和機器學習算法進行數據分析。我也更深刻地意識到了數據隱私在現今社會中的重要性，以及需要我們繼續關注隱私保護的問題。希望能夠在未來的工作中應用這些知識，繼續為隱私的保護做出貢獻。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 游雅晴 |
| 業師名稱 | 張致恩 博士 | 學號 | 408261357 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 教授今天講的內容主要是在介紹資料庫如何運用一些技巧保護隱私，因為資料庫可能遭到有心人士入侵，造成資料外洩。我們可以使用random noise來保護隱私，將資料加上random noise，讓資料盡量相同，減少差異，就可以達成因差異造成的資料特殊性，但同時random noise也有條件限制，不能太大或太小，且必須隨機，若使用常數就很容易被破解。<br><br>教授有講解範例，讓我們比較容易理解問題，其中有提到Binary Mechanism，即回答只有yes或no，但是我們無法確保回答是否正確，因此教授也提到了一種特殊的解決方法，即”合理的否認”，當user不信任Data curator時，即可否認。其實現今的資安問題日漸嚴重，對資安長的需求也越來越多，隨著科技的發展，資安問題也是不可忽視的一環，所以今天聽了教授的演講覺得還蠻新奇的，學校比較少有講解實務上如何去處理資安問題，大部分都是講解理論，但對於即將與職場接軌的我們還是應該多了解實務上的操作，也需要我們自己多去探索，畢竟讀書與實作還是兩回事。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 蔡崴翔 |
| 業師名稱 | 張致恩 博士 | 學號 | 409261184 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 這次的演講內容比預想的還有深度，學習到了很多之前沒有聽過的知識，一開始所提到的Differential Privacy是一個非常重要的隱私保護概念，在保護個人數據的隱私之外，同時仍允許研究者從這些數據中提取有用的統計訊息。Differential Privacy可以通過引入噪音，來達到隱私保護的目的。這種方法的基本思想是在原始數據中加入一些隨機噪音，以掩蓋特定個體的數據，從而確保該個體的隱私不會受到侵犯，這樣可以保證數據的隱私性，同時又不會過度影響研究的結果。<br><br>接下來提到老師有提到“Privacy budget”，在Differential Privacy的框架下，它是一個非常重要的概念。Privacy budget是一個限制條件，用於限制研究者能夠提取的數據量。簡單地說，就是研究者在使用Differential Privacy方法時，必須在Privacy budget範圍內使用隨機噪音。如果研究者使用的噪音超出了Privacy budget，就會犧牲更多的隱私。因此，Privacy budget非常重要，它可以幫助研究者在數據隱私和研究結果之間找到一個平衡點。<br><br>最後老師提到的Laplace mechanism是Differential Privacy中最常見的機制之一。該機制通過向原始數據中添加服從Laplace分布的噪音，以實現Differential Privacy。這種機制在保護隱私的同時，也可以提供比較準確的統計結果。Laplace mechanism的基本思想是將每個數據點添加一個服從Laplace分布的噪音，噪音的大小取決於數據的靈敏度和Privacy budget。<br><br>Differential Privacy技術在實際應用中有著廣泛的應用。例如，在醫療保健領域中，我們可以使用Differential Privacy技術對病人數據進行分析，提取有價值的醫學信息，同時保護病人數據的隱私。在社交網絡中，我們可以使用Differential Privacy技術對用戶行為進行分析，提取有價值的社交信息，同時保護用戶的隱私，總結來說，這是一個非常實用的技術。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 高楷昇 |
| 業師名稱 | 張致恩 博士 | 學號 | 408261773 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 在這次的演講中，張致恩博士為我們介紹了「differential privacy」這一重要的概念。雖然我並沒有完整聆聽整場講座，但從這短暫的時間也有了一些體悟，differential privacy可以在保護個人資料的同時，讓我們得到有用的統計資訊。<br><br>在演講中，張致恩博士提到了一些差分隱私的實際應用案例，例如，地理資訊系統中的位置隱私保護和機器學習模型的訓練過程。他還解釋了如何使用一些數學工具，例如拉普拉斯機制和指數機制，來實現差分隱私。張博士用淺顯易懂的語言，讓我們更好地理解這個概念，對我們的學習有很大的幫助。他友善的態度和豐富的知識，使我深感敬佩。這次演講讓我認識到差分隱私的重要性，也讓我更加關注數據安全與隱私保護。未來，我將努力學習這方面的知識，為保護個人隱私做出貢獻。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 莊緗柔 |
| 業師名稱 | 張致恩 博士 | 學號 | 409261342 |
| 時　間 | 112 年 4 月 26 日 ( 三 ) AM 09:00 – AM12:00 | | |
| 學生心得 | Differential Privacy (差分隱私)提供個人隱私相對高的保障，利用數學框架，確保數據集中的個人隱私，不洩漏數據集中任何個人的敏感訊息的情況下分析數據。運作機制是提供足夠的 noise 給 output。自己是第一次知道 differential privacy，所以特別印象深刻，增加個人隱私資料在網路上相對安全的措施，主要用於統計資料，查詢集合裡面的特定族群，在收集群體資料時同時能夠保護個人用戶的 data，加入 epsilon 來表示隱私保護程度，屬於隨機性的參數，因此在 DP 中數據可用性和隨機保護構成一個 trade-off。此外，聽完演講後，我上網查了一下業界在 DP 的運用，APPLE 公司在 2016 年就把 DP 技術使用在手機用戶端中，其中使用了 3 個 DP 數據搜集架構，Private Count Mean Sketch(CMS)、Private Hadamard Count Mean Sketch (HCMS)、Sequence FragmentPuzzle (SFP)。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 陳冠宇 |
| 業師名稱 | 張致恩 博士 | 學號 | 408262519 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 經過這次張博士的演講，我能初步的了解differential privacy 的作用跟應用方法，畢竟現在經過科技、人權的快速發展，取得資料的速度更快、更方便，而人們對於保護自己隱私的意識也越來越高，所以對數據進行分析和共享時，必須保護個人隱私並提供有用的統計分析資料，但這些也都是理論上的概念，如果要真正實施這個理想還要有其他特殊的算法 Eg. 加噪算法、打散算法...等，以達到兩者的平衡，而演講得當下我也有查一些資料關於differential privacy 的實際應用例子。<br><br>第一個例子是在疫情的追蹤: 經過這兩年多的疫情肆虐下，被追蹤足跡已竟不是一件感到令人意外的一件事情，所以為了保護個人隱私，數據通常需要經過差分隱私的處理,在數據中增加一些隨機噪聲,使單個使用者不會被精準的追蹤,同時提供有用的分析結果。<br><br>第二個例子是近年來大受網路用戶歡迎的社交網路平台,為了提供更好的服務和廣告定向，數據裡面會有大量的敏感信息，所以為了保護個人隱私，所以使用差分隱私技術，對資料進行加噪或打散處理，以免用戶信息洩漏。<br><br>經過兩次的演講能夠完全知道現在人對於自己在網路上的隱私權,有多大的重視跟保護,讓我也覺得說,好像很多隱私宣導是必要的,而不是說說口號而已,以後再對於自己的帳戶密碼、資料，都會多一點資安的保護，八瓜以後寫的程式也是如此。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 林家明 |
| 業師名稱 | 張致恩 博士 | 學號 | 408262765 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 這次演講主要在講述如何保護受訪人回答的隱私問題，例如講師用比較敏感的六個月內有沒有吸過大麻這個問題，這時候會通過馬賽克的方式來替受訪人的問題做一些加密，以防止外部的人取得這項數據時可以輕鬆地獲得採訪資料，而採訪者可以經由正確的解碼方式，來獲得最接近的答案，我認為這次的演講題目非常的新穎，沒有想到做一個問卷調查也需要考慮到資安的問題，也讓我了解到了資料安全性的重要。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 林品瑄 |
| 業師名稱 | 張致恩 博士 | 學號 | 408261668 |
| 時　　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 聽了這次的講座，差分隱私的用意是如果我們隨意的去修改資料庫裏面的紀錄，當時統計出特徵就沒辦法反推單一紀錄裡面所有的內容。我覺得隱私是必須設定不公開的，這樣很容易被駭客破壞。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 杜懷豫 |
| 業師名稱 | 張致恩 博士 | 學號 | 408262090 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 這次的演講，除了演講的內容以外，有一件特別令我印象深刻的事，講師在講課時，出現了一個詞，叫做Plausible deniability，講師問我們，這個詞在這裡是甚麼意思，並讓我們上網查，雖然一查就查到結果了，意思是合理推諉，或稱作似是而非的否認，但這個結果如果放在演講的那段文字裡，顯得有些奇怪，後來老師告訴我們，那個詞可以是模稜兩可的意思，這並不是很罕見的詞彙，但我們沒有想到，也許在英翻中的部分，除了普通的翻譯，也需要經過一些合理性的思考，尋找其他意思相近且更為合理的詞彙。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 吳佳穎 |
| 業師名稱 | 張致恩 博士 | 學號 | 409261134 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 資訊安全是現代社會中非常重要的一環,因為我們在日常生活中越來越依賴資訊科技，包括網路、手機、電腦等，因此資訊安全成為必須要關注的議題。教授提到了不同的概念和技術，包括differential privacy, random noise等。這些概念和技術都是為了保護個人隱私和敏感資訊而存在的。<br><br>Differential privacy(差分隱私)是一種保護個人隱私的技術，它通過向數據中添加隨機噪音來保護數據中的個人信息。差分隱私還提供了一個privacy budget(隱私保護參數)，用於評估數據共享所涉及的隱私風險。而random noise(隨機噪音)是一種通過在數據中添加隨機的noises,使得外界無法得知數據的真實價值的技術。可以用於數據共享和數據挖掘等領域，保護個人隱私和敏感資訊。教授還說明比較了differential privacy (差分隱私)和local differential privacy (局部差分隱私)之間的區別。LDP是一種針對單個用戶的隱私保護技術，而DP則是一種針對數據集的隱私保護技術。兩種技術都可以用於保護個人隱私，但其實現方法和適用場景不同。<br><br>這些概念和技術都非常重要，可以幫助我們更好地保護個人隱私和敏感資訊。隨著資訊科技的發展和數據應用的普及，個人隱私面臨的威脅越來越多，因此我們需要學習和應用這些技術，以確保個人隱私和敏感資訊的安全。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 張嘉玲 |
| 業師名稱 | 張致恩 博士 | 學號 | 407261659 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 今天很開心能夠聽到此演講，了解到參數大小會影響到便是的結果，聽了後才知道即了解這有關資訊安全的部分。感謝有這次課堂上的時間能夠聽演講希望下次還有別的演講可以聽可以去拓展自我視野。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 林俞駿 |
| 業師名稱 | 張致恩 博士 | 學號 | 409262396 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 這次演講講到了有關怎麼把數據加上noise，讓資料中的隱私不會洩漏出去，雖然剛開始時聽得確實很模糊，什麼plausible deniability，查翻譯是說"似是而非的否認"，後面理解了是讓資料加上noise之後可以有一種不確定性，像是我們在回答一個有點讓人不好意思地回答時，加上這麼一個不確定，在別人問起時也可以否認掉，這次演講也讓我學到了很多東西。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 邱晉寬 |
| 業師名稱 | 張致恩 博士 | 學號 | 409261079 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 作為一名資工系的大學生，我對於差分隱私框架、隱私預算以及拉普拉斯機制有一些心得體會。<br><br>差分隱私框架的出現為保護數據隱私提供了一個全新的方法。傳統上，數據隱私通常是通過加密、存儲和傳輸等方式進行保護，但這些方法往往存在漏洞，容易被攻擊者破解。而差分隱私框架通過在數據處理過程中添加一定量的隨機噪聲，從而達到保護數據隱私的目的。這種方法不僅可以保護數據隱私，還可以確保數據的準確性。<br><br>隱私預算是差分隱私框架中非常重要的概念。隱私預算表示在一定範圍內可用於添加隨機噪聲的數量，通常以一個正數來表示。隱私預算越大，可以提供更好的隱私保護，但同時也會對數據的準確性產生影響。因此，在使用差分隱私框架時，需要根據實際情況來選擇適當的隱私預算。<br><br>最後，拉普拉斯機制是差分隱私框架中最常用的添加隨機噪聲的方法之一。拉普拉斯機制通過向原始數據添加服從拉普拉斯分布的隨機噪聲，從而實現數據的隱私保護。這種方法不僅保護數據隱私，還可以確保數據的可用性。然而，在使用拉普拉斯機制時，需要注意噪聲的大小，過大或過小的噪聲都會對數據的準確性產生影響。<br><br>差分隱私框架、隱私預算以及拉普拉斯機制是保護數據隱私的有效方法。在實際應用中，我們需要根據具體情況來選擇合適的方法和參數。另外，Differential privacy framework也非常重要，它是一個旨在保護個人敏感信息的隱私保護框架，可以在不犧牲數據可用性的情況下提供保護。在Differential privacy framework中，數據被修改以確保輸出不會揭示任何關於個人的信息。這種修改是通過添加噪音來實現的，而Privacy budget則是用來控制添加噪音的量。Laplace mechanism是一種實現差分隱私的方法，它使用Laplace分佈來添加噪音，以保護數據的隱私。Laplace mechanism通常用於對連續數據進行噪音添加。<br><br>這三個主題在當今的數據科學領域中都非常重要，它們可以幫助我們保護敏感數據的隱私，同時保持數據的可用性。作為一名資工系的大學生，我認為了解這些主題的重要性，並學習如何應用它們，將有助於我們成為更有價值的數據科學家和計算機專業人員。 | | |

| 學生演講心得記錄 | | | |
|---|---|---|---|
| 演講主題 | Introduction to differential privacy | 學生姓名 | 李維琪 |
| 業師名稱 | 張致恩 博士 | 學號 | 409261627 |
| 時　間 | 112　年　4　月　26　日（三） AM 09:00 – AM12:00 | | |
| 學生心得 | 上禮拜在課堂中老師邀請了張致恩博士來演講，演講主題是介紹differential privacy，同時也介紹了Randomized Response的使用、以及隱私和效用之間的平衡。<br><br>在演講過程中，張致恩博士介紹了幾種保護隱私的方法。其中DP和LDP是兩種比較常用的方法。DP是一種強隱私保護技術，可以通過添加噪聲的方式使得數據無法被逆向推斷，但這種方法會對數據的精度和可用性產生一定的影響。而LDP是一種更加輕量級的技術，它可以在一定程度上緩解DP帶來的精度問題，但同時也會增加一些隱私泄露的風險。他也叫全班試著上網搜尋並試著用自己的話說出DP和LDP的差別，雖然這兩個名詞並非初次見到，但藉由張博士的講解，我對它們有了不同層面的理解。<br><br>張致恩博士還介紹了隨機響應（randomized response）這種方法，它可以通過對回答做出隨機的扭曲來達到保護隱私的效果。這種方法比較適用於一些離散的場景，但也有一些局限性。在講解中，張致恩博士還提到了隱私和效用之間的權衡。在實際應用中，我們經常需要在保護隱私和維護效用之間做出取捨。一方面，保護隱私是非常重要的，但另一方面，如果對數據進行了太多的扭曲，可能會對數據的可用性和精度造成影響，進而影響到應用的效果和價值。<br><br>此次的演講使我受益良多，讓我對差分隱私、局部差分隱私、隨機響應等技術有了更深入的了解，講者透過簡單的例子來讓我們對這困難的學術知識有進一步的認識。 | | |