國立臺東大學 理工學院
NATIONAL TAITUNG UNIVERSITY COLLEGE of SCIENCE and ENGINEERING

教師指導學生專題製作與論文競賽補助 成果報告

一、 申請補助計畫基本資料

申請教師	陳志全	核定經費	7000
單位系所	資訊管理學系	經費執行情況	☑已請購核銷完畢 □尚未請購核銷 □經費餘款_____
計畫執行年度/學期	113 年度	參賽期程	113 年 1 月 1 日~ 113 年 12 月 31 日
參加競賽/學術活動名稱	1. 通過國科會大專生計畫 2. 2024 資訊管理暨電子商務經營管理研討會發表論文	作品名稱	1. 資訊化時代下的資安問題ー基於 GAN 生成對抗網路之惡意攻擊偵測模型 2. 應用主題模型分析 108 課綱與城鄉差異對學生之影響
指導參賽學生姓名	1. 張焱凱 2. 曾嚴霆、鍾佳妤、王宥蓁、張焱凱	班級	1. 綠資三 2. 綠資三、綠資四
競賽性質	□國際性 ☑校際 □校內(院級以上)	參賽地點	1. 無(非競賽(國科會)) 2. 臺東大學
系所主管簽章		日期	
學院院長簽章		日期	

一、 參賽作品：(論文摘要或作品說明)

作品1摘要:

隨著人們在線上活動的時長增加，個人資訊的價值也日益提高。資訊安全的不足可能導致個人隱私的侵犯，影響社會信任和穩定。網路釣魚、惡意軟體、以及大規模的資料洩漏事件，都讓人們對個人資訊的安全感到擔憂；而現代經濟體系高度依賴資訊技術和資料流通，企業在運營中存儲著龐大的資料，包括客戶資訊、營運資料等，這些資料的安全直接關係到企業的競爭力和穩定性。大規模的資料洩漏和駭客攻擊可能對企業造成重大損害，也可能影響整個經濟體系的運作。

本專題研究將以現今社會高度依賴資訊科技，在進行網路活動時如何預防巨大的資安問題做為發想研究題目,透過訓練生成器和判別器，以生成器生成逼真的樣本，而判別器則設計為區分真實的樣本和生成的樣本，這兩者在訓練過程中相互對抗，使得生成器生成的樣本越來越逼真，而攻擊者則使用這些訓練好的生成器生成對抗樣本，這些樣本在表面上可能與真實樣本極為相似，但都添加了微小擾動。之後，生成的對抗樣本將會被提交至目標模型進行預測或分類。最後，攻擊者會評估目標模型在對抗樣本上的預測，如果目標模型在對抗樣本上出現錯誤的預測，則攻擊被視為成功，而後，即可得知目標模型在安全性上是否存在漏洞。

關鍵字:GAN，對抗式攻擊，對抗樣本，圖像分類器

作品2摘要:

如今教育改制不斷，學生學習學科內容以外，也需對課外知識內容做延伸學習，舉凡來說，由中學生網站舉辦的小論文競賽，讓全台高中生提前學習做研究，針對題目進行深度的探討，然而時代變化和十二年國教的推動下，學生選定小論文研究主題時，也需關切新興議題以及拓展不同研究方向。

本研究收集108課綱實施後的小論文得獎作品，從中分析五年六都與非六都的學生作品，與教育部提出的19個議題學習目標是否切合，並觀察兩者有無因地區產生的差異。運用主題模型(Topic Model)與機器學習(Machine Learning)，將小論文作品標題拆解，找出符合議題學習目標的關鍵字，觀察與推論分類結果，找出導致城鄉差異的原因，及兩者的學生作品是否與19個議題學習目標契合。

關鍵詞：十二年國教、自然語言處理、文字探勘、深度學習、主題模型

二、 參加之競賽活動：(請依據參加活動次數，附上相關活動簡章或海報、議程與參加證明等佐證資料)

1. 國科會網站(https://www.nstc.gov.tw/)

2. 國立臺東大學辦理「2024 資訊管理暨電子商務經營管理研討會(2024IMECM)」及論文投稿(研發處公告)(網址：https://research.ntou.edu.tw/p/406-1021-96350,r1057.php?Lang=zh-tw)

三、 參賽準備與活動記錄

1. 本年度專題生參加 2 項活動:國科會大專生研究專題計畫，由綠資三年級同學張焱凱提出申請，該計畫每年 2 月中以前收件，焱凱同學於前一學期即開始進行，並於寒假期間完成計畫撰寫。主要是利用 GAN 對抗神經網路進行假圖像的判別，對現今生成式 AI 技術進步，對人類產生助益的同時，也被非法使用進行破壞的活動，假圖像的辨識是重要的研究議題，焱凱同學於本年度積極進行研究，其成果也將發表於適合的研討會及期刊。
2. 綠資四曾嚴霆、鍾佳妤、王宥蓁、與綠資三張焱凱共同投稿並參加「2024 資訊管理暨電子商務經營管理研討會(2024IMECM)」。由綠資四鍾佳妤同學發起, 召集學程三、四年級志同道合的同學參加，以「應用主題模型分析 108 課綱與城鄉差異對學生之影響」的為題的論文獲得接受，並口頭發表。本論文運用主題模型(Topic Model)與機器學習(Machine Learning)，將高中生小論文作品標題拆解，找出符合議題學習目標的關鍵字，觀察與推論分類結果，找出導致城鄉差異的原因。專題小組同學各司其職且互相合作討論，努力完成資料分析與論文撰寫。

四、參加競賽成果 (參賽證明、得獎證明或學生心得)

1. 獲得國科會大專生專題研究計畫通過.

系所	學生姓名	計畫名稱	指導教授	核定金額
資訊工程學系	丁敬原	以區塊鏈為基礎建構金融智慧身分驗證機制	吳信德	48,000元
	張簡珈昱	校園安全行為辨識	胡舉軍	48,000元
	張凱婷	基於生成式AI之社交工程演練分析	王忍成	48,000元
	方俊翔	具動態適應性之邊緣人工智慧農作物監測	黃駿賢	58,000元
	李彩嶸	基於高光譜影像之河川汙染指數分類	楊弘章	58,000元
	林郁潔	具高光譜影像之邊緣人工智慧河川汙染監測 Edge AI-based river pollution monitoring with hyperspectral imaging	黃駿賢	58,000元
	楊家宥	沈浸式語言互動與文化傳承:利用大型語言模型(LLM)於 3D 虛擬實境中傳播臺灣原住民文化的創新教學策略	賴盈勳	48,000元
應用科學系	吳昱煒	探索圓偏振光控制四苯乙烯 對映選擇之研究	王順發	48,000元
	曾仲廷	準二維鈣鈦礦與奈米晶體混成薄膜之光電特性探討	黃俊元	48,000元
	林柏州	以鈷化合物為催化中心，探討亞硝酸還原成一氧化氮反應	李建明	48,000元
	江羿樺	利用碳-氫鍵活化策略合成雙(聯苯基)取代雙吡唑并[1,5-a]吡啶暨環糊精包覆作用下之聚集誘導放光性質研究	朱見和	48,000元
生命科學系	李祐德	探討抗電磁波奈米素材四氧化三鐵在蓖麻蠶絲的應用	呂佩倫	58,000元
	沈鈺成	利用液化澱粉芽孢桿菌 Bacillus amyloliquefaciens HS3 分離株提升番茄對於炭疽病菌的防治效果	黃祥恩	48,000元
資訊管理學系	張焱凱	資訊化時代下的資安問題─基於GAN生成對抗網路之惡意攻擊偵測模型	陳志全	51,000元
	賴士勳	具低成本考量之海洋教育數位模組：以東部地區國中小學教學應用為例	謝昆霖	51,000元
綠色與資訊科技學士學位學程	吳柏慶	考慮溫度效應之止推滑塊軸承的熱液動潤滑解析解及潤滑特性分析並推導可供業界使用的公式	朱力民	48,000元
	溫晨楷	結合萊維飛行與S型函數之改良型蜜獾演算法應用於動力電池參數辨識研究	劉恩睿	58,000元
生物醫學碩士學位學程	羅翊瑄	天然核酸雜合奈米膠在抗發炎水膠的製備	陳宇楓	48,000元
高齡健康與照護管理原住民專班	陳淀潢	利用影像辨識技術輔助懷舊治療進行之研究	陳育嫻	48,000元

2. 「2024 資訊管理暨電子商務經營管理研討會(2024IMECM)」論文發表證明

2024 資訊管理暨電子商務經營

管理研討會

鄭亦君、曾嚴霆、鍾佳妤

王宥蓁、張焱凱、陳志全

參與 2024 資訊管理暨電子商務經營

管理研討會發表論文

應用主題模型分析 108 課綱

與城鄉差異對學生之影響

特頒此證

籌備委員會主席 謝昆霖

2024 資訊管理暨電子商務經營管理研討會籌備委員會

中華民國 113 年 05 月 10 日

National Taitung University