



112 年度委託研究報告

跨領域應用規劃計畫委託研究採購案 期末報告

計畫編號：FY112

執行單位：財團法人工業技術研究院

版別：第 2.0 版

技資編號：521B20026

計畫委託機關：數位發展部

中華民國 112 年 12 月



112 委託研究報告

GRB 系統編號：PG11202-0217

跨領域應用規劃計畫

受委託單位

財團法人工業技術研究院

計畫主持人

王邦傑

共同主持人

卓傳育

研究人員

林咨銘、陳彥學、黃信騫、高銘智、羅翊萍、楊惠國、
林育生、張文村、蔡宜學、徐櫻真、王晟宇、簡文君

研究期程：中華民國 112 年 2 月至 112 年 12 月

研究經費：新臺幣 3,144 萬 5,615 元整

本報告不必然代表數位發展部意見

中華民國 112 年 12 月



目錄

目錄.....	I
表次.....	IV
圖次.....	VIII
摘要.....	XVI
Abstract.....	XXIV
第一章 緒論.....	1
第一節 計畫背景	1
第二節 計畫架構	3
第三節 計畫執行內容	4
第四節 6G 關鍵技術指標	7
第五節 研究方法	11
第六節 預期成果	16
第七節 計畫執行狀況	18
第二章 建立 6G 跨領域應用情境之參考架構先導評估.....	27
第一節 6G 應用標準趨勢與進程	29
第二節 蒐集研析 Cloud-Native 6G 及 AI-Native 6G 之跨領域應 用情境參考架構	45
第三節 跨應用層和網路層的通訊強化機制研析與方法	87
第四節 跨領域應用情境實證與離型系統先導評估	92
第五節 小結	113
第三章 規劃與建立安全與可靠的 6G 跨領域應用機制與技術 先導 評估.....	117
第一節 發展容錯技術強化服務韌性	119
第二節 分散式及大量裝置(Massive AIoT)的安全議題研析 ...	141
第三節 跨領域應用情境的安全與可靠實證先導評估	147



第四節 小結	159
第四章 建立 6G 應用自動攻防與情資離型系統先導評估	163
第一節 建立 6G 應用自動攻防與情資離型系統說明	164
第二節 滲透測試規範蒐集研析	168
第三節 6G 應用服務層之偵防工具化可行性評估	177
第四節 可支援 6G 網路威脅訊結構	203
第五節 6G 應用自動攻防與情資離型系統情境實證先導評估	214
第六節 小結	232
第五章 6G 資安產業研析與防護實證應用驗測先導評估	237
第一節 全球 Pre-6G 資安技術發展趨勢	239
第二節 探討我國 6G 資安服務框架與推動機制	254
第三節 6G 資安產業研析與防護實證應用驗測實證先導評估	260
第四節 6G 資安產業研析座談會	297
第五節 小結	309
第六章 維運公部門連結小組	312
第一節 辦理公部門連結小組會議	313
第二節 協助國際標準組織參與及建立國際合作管道/案例	320
第三節 觀測國際應用服務展及國內產業能量盤點	322
第四節 小結	327
第七章 研析與實證成果	329
第一節 跨領域應用	329
第二節 資安產業研析	332
第三節 維運公部門連結小組	334
第八章 結論與建議	335
第一節 短期可行建議	335



第二節 中長期建議	336
第三節 計畫 4 年執行架構	337
第四節 其他建議持續關注議題	347
參考資料.....	349
中英文名詞對照	358
附件資料.....	367
附件一、常駐履約人員工作項目	367
附件二、6G 資安產業研析座談會	374
附件三、公部門連結小組電子報	398
附件四、公部門連結小組第 1 次會議會議紀錄	409
附件五、公部門連結小組第 2 次會議會議紀錄	437
附件六、公部門連結小組第 3 次會議會議紀錄	475
附件七、公部門連結小組第 4 次會議會議紀錄	493



表次

表 1、6G 關鍵性需求 KPI	7
表 2、6G 關鍵性技術指標對應表	9
表 3、計畫進度甘特圖	18
表 4、期中期末工作量化指標與質化產出	20
表 5、容器技術及虛擬機器技術特性比較	52
表 6、Kubernetes 容器管理平臺特點	55
表 7、Docker Swarm 容器調度管理平臺特點	56
表 8、Kubernetes 和 Docker Swarm 比較	58
表 9、VMware vSphere 虛擬機器管理平臺特點	59
表 10、VirtualBox 虛擬機器管理平臺特點	60
表 11、Microsoft Hyper-V 虛擬機器管理平臺特點	62
表 12、Xen 虛擬機器管理平臺特點	64
表 13、虛擬機器管理平臺特點比較	65
表 14、開源軟體應用一覽表	88
表 15、Server 軟硬體規格	99
表 16、Client 軟硬體規格	100
表 17、參數調整對應準確率及時間	105
表 18、CNN 與 CIL 演算法舊/新類別準確率與時間比較	108



表 19、CNN 與 CIL 正確率皆較低之案例(CNN<90% CIL<90%)	110
表 20、CNN 正確率較低 CIL 正確率正常案例(CNN<90% CIL>90%)	111
表 21、CNN 正確率正常 CIL 正確率較低案例(CNN>90% CIL<90%)	112
表 22、實體主機規格	150
表 23、5G 核心站點虛擬主機規格	151
表 24、MEC 平臺虛擬機器規格	151
表 25、UE 虛擬機器規格	152
表 26、測試 1-評估分散式管理機制	152
表 27、測試 2-評估容器監看回復機制	153
表 28、測試 3-評估分散式儲存系統	153
表 29、應用層滲透測試項目與基準	170
表 30、網路層滲透測試項目與基準	173
表 31、感測設備層滲透測試項目與基準	174
表 32、5G 和 6G 網路切片區別一覽表	183
表 33、實證軟硬體說明	222
表 34、測試資料集	226
表 35、AI 攻擊測試步驟-訊號擾動對抗性攻擊工作流程表	228



表 36、AI 攻擊測試步驟-策略滲透對抗性攻擊工作流程表	229
表 37、AI 攻擊實測結果	231
表 38、4 種攻擊類型之緩解措施與 ISO 27001：對應控制項目組	264
表 39、6G 網路模擬器軟硬體規格	271
表 40、Pre-6G AMF 的 N1 介面攻擊測試項目	279
表 41、Synchronization failure handling	280
表 42、RES* verification failure handling	281
表 43、Replay protection of NAS signalling messages	281
表 44、NAS NULL integrity protection	281
表 45、NAS integrity algorithm selection and use	282
表 46、Bidding down prevention in Xn-handover	282
表 47、5G-GUTI allocation	283
表 48、Invalid or unacceptable UE security capabilities handling	283
表 49、「Pre-6G AMF 的 N1 介面攻擊」測試結果	290
表 50、112 年度電子報填報概況	323
表 51、頻段需求現況調查表	324
表 52、各工作組研討座談會調查表	325
表 53、113 年公部門連結小組舉辦國際研討會調查表	325
表 54、112 年度國際會議參與後調查表	326
表 55、113 年度國際會議參與調查表	326



表 56、每月電子報發報列表	367

表 57、每月工作會議討論重點	372



圖次

圖 1、計畫架構圖	3
圖 2、6G 使用情境與系統發展架構	35
圖 3、Nokia 發布 6G 標準演進時程	41
圖 4、Ericsson 發布 6G 標準規劃時程	41
圖 5、Qualcomm 發布 6G 標準規劃時程	42
圖 6、LG 發布 6G 標準規劃時程	43
圖 7、SONY 發布 6G 標準規劃時程	44
圖 8、單機式架構圖	50
圖 9、容器技術架構圖	50
圖 10、虛擬機器技術架構圖	51
圖 11、傳統容器管理模式	53
圖 12、Kubernetes 容器管理模式	55
圖 13、全虛擬化技術	63
圖 14、半虛擬化技術	64
圖 15、6G 資料管理架建構議	79
圖 16、6G 之 AI-Native 融合架構考量	80
圖 17、6G 之 AI-Native 3 個要素面向	81
圖 18、聯合學習面臨的問題	84
圖 19、跨領域物件辨識應用——智慧商店	85



圖 20、跨領域物件辨識應用——醫院疾病診斷系統	86
圖 21、COIL 演算法	94
圖 22、最佳傳輸演算法	95
圖 23、模型應用示意圖	96
圖 24、上傳資料示意圖	97
圖 25、產品內容統整示意圖	97
圖 26、跨領域應用情境實證與雛型系統-應用情境架構示意圖	99
圖 27、跨領域應用情境實證與雛型系統-測試步驟示意圖	102
圖 28、商品資料集學習率	103
圖 29、商品資料集	106
圖 30、Task 正確率比較圖	107
圖 31、準確率區間比較圖	107
圖 32、瑞擎數位 MEC 開道器規格	119
圖 33、MQTT 協定示意圖	121
圖 34、雲端、霧、邊緣運算架構演進示意圖	123
圖 35、MEC 示意圖	124
圖 36、MEC IoT 應用場景	126
圖 37、MEC CDN 快取機制	127
圖 38、MEC IoT 應用場景	128
圖 39、BC 工作流程	130



圖 40、DLT 參考架構.....	132
圖 41、PDLF 於行動網路之示意圖	133
圖 42、BC 資料分享使用例.....	134
圖 43、BC 加入新區塊過程.....	135
圖 44、BaaS 系統架構.....	136
圖 45、發布/訂閱模式示意圖	138
圖 46、中央式代理者結構(a)、分散式代理者結構(b).....	139
圖 47、Blockchain of Things 概念圖	140
圖 48、分散式儲存系統示意圖	143
圖 49、去中心化管理機制運作	145
圖 50、系統階層圖示意圖	146
圖 51、BC 驗證流程示意圖	148
圖 52、基礎環境示意圖	149
圖 53、跨領域應用情境的安全與可靠實證測試系統架構圖	150
圖 54、認證延遲時間比較圖	154
圖 55、情境 A 與情境 C 比較圖.....	155
圖 56、情境 B 與情境 D 比較-節點共識示意圖	155
圖 57、包含重啟的認證延遲時間	156
圖 58、IoT 代理者群組吞吐量	157
圖 59、分散式系統存取時間	158



圖 60、5G 與 6G 在網路威脅的差異	164
圖 61、從網路特性與應用面比較 5G 與 6G 的資安需求	166
圖 62、5G 核網參考測試架構	169
圖 63、網路切片的工作原理	181
圖 64、網路切片攻擊原理	184
圖 65、IP Spoofing 攻擊的工作原理	187
圖 66、DoS 攻擊的工作原理	193
圖 67、DrDoS 攻擊的工作原理	195
圖 68、TLS Downgrade Attack	199
圖 69、STIX 的使用情境	203
圖 70、各層級角色權責與分工	204
圖 71、6 類資安情資種類與 10 類資安事件類型	205
圖 72、N-ISAC 情資欄位對應 STIX 2.1 物件說明(資安事件與非資 安事件)	206
圖 73、N-ISAC 情資格式架構 1	207
圖 74、N-ISAC 情資格式架構 1 驗證欄位	208
圖 75、情資分類、影響等級、分享等級	209
圖 76、情資來源範例	210
圖 77、情資編號/類型/主旨/發布時間範例	210
圖 78、分享等級範例	211



圖 79、建議措施與附件範例	211
圖 80、受駭 IP 與攻擊 IP 之 STIX 2.1 表達方式	213
圖 81、5G 與 6G 導入 AI-Native 示意圖	215
圖 82、多階段 ML 設計	218
圖 83、測試環境	219
圖 84、實證先導評估使用的 5G 環境模擬軟體	220
圖 85、傳統 DoS 攻擊的測試架構	220
圖 86、AI 攻擊測試架構	221
圖 87、傳統測試攻擊結果	230
圖 88、發動 DoS 攻擊 UE 端的平均 datarate	230
圖 89、6G 網路環境高度整合 AI、大數據分析與邊緣運算	239
圖 90、NESAS 宗旨	241
圖 91、NESAS 流程概述	242
圖 92、NESAS 測試框架	243
圖 93、SECAM 檢測流程	244
圖 94、5G 資安檢測流程	245
圖 95、NESAS 資安認證範圍	246
圖 96、3GPP 第 3 工作群組-安全性(SA3 WG)的工作規劃	248
圖 97、3GPP RAN 第 19 版本標準研討會列舉安全議題	249
圖 98、Apple 提案 RAN 端安全議題	250



圖 99、Apple 提案接取層安全性增強	251
圖 100、Google 新興服務重視通訊安全的工作規劃	252
圖 101、MITRE 的工作規劃	253
圖 102、模擬 6G/Pre-6G 基地臺與核網連線 2 大類型 4 種資安攻擊 情境	262
圖 103、Pre-6G 網路元件模擬器與實驗架構圖	266
圖 104、Pre-6G 網路元件模擬器與實驗架構圖	267
圖 105、Amarisoft 軟體核心網路及 gNB (左)與軟體 UE (右).....	267
圖 106、Pre-6GC 模擬器操作介面圖	268
圖 107、Pre-6G gNB 與 UE 模擬器操作介面圖	269
圖 108、Amarisoft 軟體核心網路及 gNB 規格	270
圖 109、Amarisoft 軟體 UE 規格	271
圖 110、Pre-6G SUPI/IMSI 捕捉器	273
圖 111、透過 Illegal UE 實現入網阻斷服務攻擊	273
圖 112、透過 Illegal ME 實現入網阻斷服務攻擊	274
圖 113、Pre-6G 假核心網路與 gNB 重播 AV 的安全威脅	275
圖 114、Pre-6G 假核心網路與 gNB 跳脫認證程序安全威脅-誘騙攻 擊	275
圖 115、假統一資料管理功能重播認證向量資料庫	276
圖 116、Pre-6GC 核心網路 SUPI 帳號填充攻擊實驗架構	277



圖 117、Pre-6G 核心網路用戶 SUPI 帳號填充攻擊實測驗證.....	278
圖 118、Pre-6G AMF 的 N1 介面攻擊測試實驗架構	280
圖 119、Pre-6G SUPI/IMSI 捕捉器擷取竊聽用戶的實測驗證.....	284
圖 120、夾帶 Cause(Illegal UE)的拒絕註冊訊令	285
圖 121、Pre-6G 假核心網路與 gNB 重播 AV 的實測驗證.....	285
圖 122、Amarisoft 的軟體 UE 的實測驗證	286
圖 123、Nemo Handy 的實測驗證.....	286
圖 124、Amarisoft 的軟體 UE 的實測驗證	287
圖 125、Pre-6GC 核心網路 SUPI 帳號填充攻擊器操作介面.....	288
圖 126、Pre-6G AMF 的 N1 介面攻擊測試器操作介面	289
圖 127、Synchronization failure handling (over N2) 測試	290
圖 128、RES* verification failure handling (over N2)測試.....	291
圖 129、Replay protection of NAS signalling messages 測試	291
圖 130、NAS NULL integrity protection 測試	292
圖 131、NAS integrity algorithm selection and use 測試.....	292
圖 132、Bidding down prevention in Xn-handover 測試.....	293
圖 133、5G-GUTI allocation 測試.....	294
圖 134、Invalid or unacceptable UE security capabilities handling 測試.....	295
圖 135、6G 資安產業研析 4 場座談會彙整	297



圖 136、公部門連結小組架構與分工	312
圖 137、112 年度公部門連結小組會議時程規劃	313
圖 138、電子報填報及發刊規則	323
圖 139、2030 ITU-R IMT-2030 期程	338
圖 140、IMT-2030 規劃中 6G 系統與應用應具備之能力	339

摘要

關鍵詞：跨領域應用；資安偵測防護；公部門連結小組

一、研究緣起

為提前布局跨領域應用技術，引領產業創新轉型與發展，將以應用情境研析與驗證、資安防護與偵測 2 大主軸，規劃與建構各類應用與資安情境下國內產業對應策略與協作機制，對未來第六代行動通訊 (6th Generation Mobile Networks, 6G) 實現商轉可能遭遇的問題與技術需求進行規劃與初期驗證，其中亦包含運用公部門連結工作小組，針對 6G 發展各項議題，進行跨部會協商與意見整合。

二、研究方法

本計畫以文獻分析法、訪談法、比較法等研究方法，與領域學者、技術專家交流意見。先以文獻分析法蒐集研析 AI 原生 (AI-Native) 和雲端原生 (Cloud-Native) 之跨領域應用情境、跨應用層和網路層的通訊強化機制、去中心化服務架構技術、資安威脅；並訪談彙整商用市場與資安應用之動態發展趨勢。針對各研析成果，建立跨雛型系統的基礎環境設定，並詳細說明實證效果。

三、重點成果

(一) 建立 6G 跨領域應用情境之參考架構先導評估

1. 聯合國已將 6G 標準系統正名為 IMT-2030，朝向智慧性普及、普適運算、沉浸多感媒體整合、數位孿生虛擬世界、智慧工業應用、數位醫療照料、普適連結、感測通訊整合及永續發展等 9 大應用趨勢演進。
2. 6G 從第五代行動通訊 (5th Generation Mobile Networks, 5G) 的增強行動寬頻 (Enhanced Mobile Broadband, eMBB)、大規模機器型通訊 (Massive Machine Type Communications, mMTC)、超可靠低延遲通訊 (Ultra-reliable and Low Latency

Communications, uRLLC) 的 3 大場景，擴增為沉浸通訊、超極可靠低延遲通訊 (Hyper Reliable and Low-Latency Communication, HRLLC)、巨量通訊、普及連線、AI 整合通訊及感測通訊整合等 6 大情境。

3. AI-Native 在 6G 無線通訊系統的特徵，須考量服務、能力、架構等 3 面向。可先考量其服務，是對延遲、能耗、隱私或服務體驗敏感，並從參考能力的運算與架構的設計 2 個面向，釐清其所須的 6G 網路系統功能，須注重於哪些重點需求面向。
4. 目前市場上實現 Cloud-Native 的解決方案包含虛擬化及容器化 2 種，及其延伸出的軟體服務，組織開發團隊須權衡需求及各種優缺點，選擇對應的開發工具。Cloud-Native 可實現資源調度彈性化、高可用容錯、環境部署靈活等優點，但也須面對學習曲線陡峭、雲端基礎設施依賴及安全隱私的挑戰。
5. 跨應用層和網路層的通訊強化機制研究方向，包含跨層訊息交換、跨層資源配置、優化網路路由和調度、跨層安全、隱私保護以及協同優化和學習。
6. 開源軟體如 NS-3、OMNeT++、OpenAirInterface 和 Mininet，被廣泛用於模擬跨應用層與網路層通訊的強化機制，特別是在研究 6G 通訊網路時。雖然這些軟體提供了有價值的工具來研究 6G 通訊網路，然而在特定方面存在限制，包括模型的精確性和複雜度、跨層整合的挑戰、協議和技術支援的不足，以及實驗平臺的限制。
7. 以智慧商店商品辨識新增類別應用比較卷積神經網路 (Convolutional Neural Networks, CNN) 及類別增量學習 (Class-Incremental Learning, CIL) 演算法效能。CNN 在新

類別時辨識正確率較佳，但對舊類別表現較差；CIL 則可維持穩定正確率但需較長訓練時間。故應根據需求選擇適當演算法。

(二)規劃與建立安全與可靠的 6G 跨領域應用機制與技術先導評估

1. B5G/6G 從毫米波頻段擴展到太赫茲 (THz) 頻段，導致網路營運商須布建更多基地臺等硬體設備以達相同覆蓋率，使得網路布建成本增加。此趨勢致使國際標準組織採用網路虛擬技術支持多租戶部署於白牌伺服器，以降低營運商成本。
2. 為了提升虛擬元件效能，用戶資料分享將不可或缺，國際標準組織已經開始討論如何結合邊緣運算與區塊鏈 (Blockchain, BC) 來建立去中心化的管理機制，在營運商與用戶無需事先有信任關係即可共享客戶資料。
3. 在邊緣運算環境建置 BC 系統及分散式認證機制，並與中央式認證機制比較，確實可以降低延遲，提升分散式系統建置於邊緣運算環境建的可行性。
4. 結合 BC 及星際文件系統 (InterPlanetary File System, IPFS) 開源的程式介面，開發以 BC 管控 IPFS 的檔案摘要值，結合兩者在邊緣運算環境建置分散式儲存系統，在實證計畫中發現 BC 的程式介面會降低 IPFS 存取速度，但對讀取過程影響較小且不受 BC 的節點數多寡影響，適合用於資料分享應用。

(三)建立 6G 應用自動攻防與情資雛型系統先導評估

1. 研析 6G 與 5G 在網路威脅的差異，6G 除了通訊技術的進步外，亦將在網路架構導入人工智慧 (Artificial Intelligence,

- AI)及機械學習(Machine Learning, ML)等新技術，因而需要及早發展針對 6G 網路架構 AI 及 ML 模型滲透測試規範。
2. 針對 IP 欺騙(IP Spoofing)、阻斷服務攻擊(Denial of Service, DoS)、降級攻擊(Downgrade Attack)等傳統資安威脅的研析，不僅沒有消失，反而更頻繁的發生，未來在 6G 時代也將持續存在，因而實體保護措施仍有其必要性與重要性。在 AI 原生安全性(AI-Native Security)、in-X 子網 Network Slicing Security 的研析過程，發現新型態的 AI 模型在未來 6G 時代，將引來更細緻與針對性的破壞，同時也不易被察覺，意味著及早進行研究並發展防禦 AI 模型攻擊的重要性。
 3. 對於網路威脅情資結構化資料交換格式(Structured Threat Information eXpression, STIX)的研析成果，找出目前國家資安資訊分享與分析中心(National Information Sharing and Analysis Center, N-ISAC)於資安事件的「攻擊 IP」與「受駭 IP」僅能呈現 IPv4，若攻擊或受駭 IP 為 IPv6 設備，則無法對應。有鑑於上述無法對應之問題，解決方法包含「新增 IPv6 Address Object」與「指定特定 IPv4 位址，再將 IPv6 位址放置於附件」2 種。
 4. 實證先導評估完成對未來 6G 導入無線資源分配 AI 模型的安全性評估，其結果顯示 AI 模型對於傳統攻擊無抵擋能力，保護措施仍須持續實施。實測對抗性攻擊顯示出無線資源分配 AI 模型的弱點，吞吐量(Throughput)與延遲(Latency)均遭受顯著影響，造成網路效能大幅降低。可能的防禦措施則是資料輸入模型前的過濾與偵測，並且在遭受攻擊後，重新標示攻擊樣本以訓練新模型提升應對對抗性攻擊的抵抗力。

(四)6G 資安產業研析與防護實證應用測驗先導評估

1. 臺灣現有工業電腦與伺服器廠商以及小型基地臺製造商，應強化對 3GPP 及 O-RAN Alliance 標準規格及關鍵技術之掌握，可依據開放式無線接取網路聯盟(Open Radio Access Network Alliance, O-RAN Alliance)的方案，以 GSMA 制定的 NESAS，搭配 3GPP 制定的 SCAS 來驗證產品安全性，於設計階段降低產品於商用時的資安修補成本，除了可以滿足潛在客戶資安需求外，同時亦可提升產品的國際市場競爭力。
2. 源於運用身分驗證或訪問控制機制是 6G 安全期待已久的功能，本計畫發展 2 大類型 4 種資安攻擊情境，測試攻擊發生的影響程度，並對應 ISO 27001:2022 控制措施「A.5.30 營運持續之 ICT 備妥性」、「A.8.9 組態管理」、「A.8.16 監視活動」導入建議防護作法，驗證緩解方案可行性，做為發展 6G 網路軟硬體資安技術建議。
3. 6G 專網多接取邊緣運算是未來部署 6G 企業專網的關鍵，本計畫從 5G、低軌衛星到 6G 資安議題，與國內网通設備廠商、資安業者與電信營運商，深耕從 3GPP 國際標準規格，探討遺留在行動網路中的安全問題，技術實證結果對應 6G 關鍵性技術指標可靠性(Reliability)與安全和隱私(Security and privacy)，在國內廠商參與國際組織討論會議時，回饋國內 Pre-6G 相關資安技術的前期研究與測試結果，形成國內外技術同步的正向循環。
4. 本計畫規劃資安座談會，多數業者表示隨著 5G 專網建置逐步推升，導致資安威脅增加的風險也備受關切，建議政府機構研擬 5G 延伸到 6G 建立相關資安標準規範，以多邊組織與國際先進國家發布之標準為依據，或是 6G 對應防護情

境與推動程序 SOP 機制，逐步建構通訊網路安全管理制度，以確保我國通訊環境之韌性與安全性，裨益我國業者進入國際 6G 供應鏈。

5. 參酌國際發展通訊資安趨勢及本計畫研究技術主題，完成 4 場技術交流座談會，會議中邀請包括專網維運商、系統整合、設備供應商、資安和研究機構等超過 50 家廠商(含因防疫線上參加)，取得不同參與者如何看待通訊世代的安全主題的面向，作為規劃一套具備安全基礎的 6G 服務架構之參據。

(五)維運公部門連結小組

1. 完成辦理 4 場次公部門連結小組會議，邀集經濟部技術司(原經濟部技術處)、經濟部產業發展署(原經濟部工業局)及國科會工程處共 3 個單位，針對 6G 推動上之各項議題進行探討與協調，以推動國內 6G 發展。
2. 完成 3 案協助政府或電信業者參與 6G 應用與標準國際組織，促進國際合作或交流，跨部會並串連公私部門能量參與大型國際盛事。
3. 完成發布 11 期電子報，蒐整國內外會展活動資訊，供產官學界於活動參與前可橫向連結，並提供國際資通訊最新訊息，以促進資源共享。
4. 建立 3 個資訊協作平臺，包含提供小組成員於申請實驗頻率之事前溝通管道、112 及 113 年度國際會議參與調查及 113 年國際會議辦理規劃協作溝通。

四、主要建議事項

(一)立即可行之建議

1. 本計畫既有之成果，可提供 6G 跨領域應用之公協會，作為先期規劃參考案例或提出建議規範，如台灣資通訊產業協會 TC1：前瞻行動通訊、TC3-裝置聯網工作小組、TC-5 網

路與資訊安全工作小組等，對本計畫內容成果進行定期分享，並視需求符合國際標準趨勢導向之建議或進行規範提案等。

2. 運用 Cloud-Native 結合生成式 AI 技術於通訊相關應用場域，以及基於資料隱私應用之分散式帳本技術 (Distributed Ledger Technology, DLT) 等，與相關應用領域聯盟/協會如開放電動車聯盟、區塊鏈愛好者協會，提出以銜接未來 6G 9 大應用趨勢相關技術與應用方向，交流聯盟與協會成員之建議與合作機會，槓桿本計畫研發資源共同建立前期的概念性驗證。
3. 同步上述作為與資訊分享於公部門連結小組，提供其他分項小組作為參考或促成合作，並規劃邀請國內外優秀學者、專家及新創等，於公部門連結小組進行交流。
4. 將本計畫之成果，如資安在 STIX 之建議、實證案例，在核網導入 AI 應用可能遭遇之攻擊、AI 跨領域應用之實證成果等，協助數位發展部資源管理司與相關單位(如資通安全研究院、國家傳播通訊委員會等)進行交流，及本計畫成果對主管機關提出建言或推動落實。

(二)中長期建議

1. 參考 FIDO 結合同訊應用、後量子密碼強化之技術進展與推動進程，規劃具備資安與隱私防護機制的 AI、混合式網路與 6G 通訊特性整合跨領域應用，帶動產業超前部署 6G 應用技術。
2. 持續觀測歐盟、美國與國際性組織、標準組織未來對 AI 法規、安全等，基於可信任 AI 之推動趨勢與做法，於本計畫中結合 AI 應用與安全、隱私、韌性等特色，規劃提出以 DLT、AI 應用/安全、FL 等為主軸之技術開發與驗證。



3. 持續參與 6G 跨領域應用之公協會，作為先期規劃參考案例或提出建議規範，如台灣資通訊產業協會 TC3-裝置聯網工作小組、TC-5 網路與資訊安全工作小組等，對本計畫內容成果進行定期分享，並視需求提出符合國際標準趨勢導向之建議或進行規範提案等。



Abstract

Keywords : Cross-Domain Application, Cyber Security for Threat
Detection and Defense, Pre-6G Inter-ministerial Cooperation Working
Group

1. General Background Information

To proactively position ourselves in cross-domain application technologies and lead the industry in innovation, transformation, and development, we will formulate and establish various strategies and collaborative mechanisms for domestic industries under two key areas: application scenario analysis and verification, and information security protection and detection. We will also plan and conduct initial validation for the issues and technical needs that may arise during the realization of the commercial transformation of the future 6th Generation Mobile Networks (6G).

2. Methodology

This project employs research methods such as literature analysis, interviews, and comparative analysis to engage with scholars and technical experts in the field. Initially, we use literature analysis to gather and scrutinize cross-domain application scenarios of AI-Native and Cloud-Native, communication enhancement mechanisms across application and network layers, decentralized service architecture technology, and information security threats. Additionally, we conduct interviews to summarize the dynamic development trends in the commercial market and the application of information security. Based on the analysis results, we will establish the foundational infrastructure of the cross-prototype system and provide a comprehensive explanation of the empirical outcomes.

3. Key Achievements of the Programme Include.

(1) Cross-Domain Application

- A. The ITU has officially designated the 6G system as IMT-2030, steering it towards the evolution of nine major application trends, Ubiquitous Intelligence, Ubiquitous Computing, Immersive Multimedia and Multi-sensory Interactions, Digital Twin and Virtual World, Smart Industrial Applications, Digital Health and Well-being, Ubiquitous Connectivity, sensor communication integration, and Integration of Sensing and Communication.
- B. 6G has evolved beyond the three primary scenarios of 5G, which include eMBB, mMTC, and uRLLC. It has now expanded to encompass six major contexts, which include Immersive Communication, HRLLC, Massive Communications, Ubiquitous Connectivity, Integrated AI and Communication, and Integrated Sensing and Communication.
- C. The characteristics of AI-Native in the 6G system need to be evaluated from three dimensions: service, capability, and architecture. We can start by considering its services, examining whether they are sensitive to factors such as latency, energy consumption, privacy, or service quality. Then, by referencing the capabilities of computation and the design of the architecture, we can pinpoint the key requirements that AI-Native should emphasize for its 6G network system functions.
- D. Currently, in the market, there are two types of solutions to achieve Cloud-Native: virtualize and containerize, along with their associated software services. Cloud-Native offers advantages such as flexible resource allocation, high availability, fault tolerance, and adaptable environment deployment.

- E.The research direction for communication enhancement mechanisms across application and network layers encompasses cross-layer message exchange, cross-layer resource allocation, optimized network routing and scheduling, cross-layer security, privacy protection, and collaborative optimization and learning.
- F.Open-source software like NS-3, OMNeT++, OpenAirInterface, and Mininet are extensively employed for simulating communication enhancement mechanisms across application and network layers, particularly in the context of researching 6G communication networks. While these software tools offer valuable resources for the study of 6G communication networks, they do have certain limitations in specific areas, including model accuracy and complexity, challenges related to cross-layer integration, insufficient protocol and technical support, and constraints in experimental platforms.
- G.Compare the performance of Convolutional Neural Networks (CNN) and Class-Incremental Learning (CIL) algorithms in identifying new product categories in a smart store. CNN exhibits superior accuracy in recognizing new categories but performs less effectively with existing ones, while CIL maintains stable accuracy at the cost of longer training time. The choice of algorithm should be based on specific requirements.
- (2)Secure, Reliable and Trusted Distributed Computing Planning.
- A.The expansion of B5G/6G into the THz frequency range has necessitated network operators to deploy more hardware equipment, including base stations, in order to maintain the same coverage. This increase in network deployment costs has

prompted international standards organizations to embrace network virtualization technology, enabling multi-tenant deployments on white-label servers, with the aim of reducing operational expenses for operators.

B.To enhance the efficiency of virtual components, user data sharing is crucial. The ISO has initiated discussions on integrating edge computing and blockchain to establish a decentralized management mechanism. This allows operators and users to share customer data without the need for a pre-existing trust relationship.

C.Establishing a blockchain system and a decentralized authentication mechanism within an edge computing environment can effectively reduce latency and enhance the feasibility of deploying decentralized systems in edge computing environments when compared to centralized authentication mechanisms.

D.By integrating the open-source program interfaces of blockchain and the InterPlanetary File System (IPFS), we developed a system where blockchain manages the file digest values of IPFS. These two technologies were combined to create a decentralized storage system within an edge computing environment. In the pilot project, it was observed that the blockchain's program interface could slow down the access speed of IPFS. However, its impact on the reading process was minimal and unaffected by the number of blockchain nodes, making it suitable for data sharing applications.

(3)6G Threat Detection and Defense

A.Analyze the differences in network threats between 6G and 5G. In addition to advancements in communication

technology, 6G will introduce new technologies such as AI and ML into the network architecture. Therefore, there is an early need to develop penetration test specifications for AI and ML models within the 6G network architecture.

- B. The analysis of traditional information security threats, such as IP Spoofing, Denial of Service (DoS), and Downgrade Attack, has not only not disappeared but is occurring more frequently. These threats will persist in the 6G era, emphasizing the continued importance and necessity of physical protection measures. In the process of analyzing AI-Native Security and in-X subnet Network Slicing Security, it has been discovered that new types of AI models will lead to more sophisticated and targeted attacks in the future 6G era, making them difficult to detect. This underscores the importance of conducting early research and development to defend against AI model attacks.
- C. The analysis results of STIX format for network threat information reveal a limitation in the (N-ISAC when dealing with "attack IP" and "compromised IP" during cybersecurity incidents. They can only present IPv4 addresses, and cannot handle IPv6 devices. To address this issue, two solutions are proposed: adding an 'IPv6 Address Object' and specifying a particular IPv4 address while including the IPv6 address in the attachmen
- D. The assessment of the security of AI models for future 6G-enabled wireless resource allocation has been completed. The results indicate that AI models are vulnerable to conventional attacks, and therefore, continuous security measures are necessary. Adversarial tests have exposed weaknesses in the wireless resource allocation AI model, leading to a substantial decrease in network performance, affecting both throughput

and latency. Possible defense measures include pre-model data filtering and detection. After an attack, re-labeling attack samples can be used to train new models, enhancing their resistance to adversarial attacks.

(4) 6G Network Element and Communication Cyber Security

Detection

A. Taiwan's existing industrial computer and server manufacturers, along with small base station manufacturers, should enhance their understanding of the 3GPP and O-RAN Alliance standard specifications and key technologies. They can adopt the O-RAN Alliance's approach, utilizing the NESAS developed by GSMA and the SCAS established by 3GPP for product security validation. This approach reduces the cost of security patches during the commercialization stage and enhances the competitiveness of their products in the international market. In addition to meeting the security requirements of potential customers, it also improves the overall appeal of their products.

B. Given the long-anticipated importance of identity authentication and access control mechanisms in 6G security, this project has developed two major categories of four security attack scenarios to assess the impact of these attacks. It also recommends protective measures in alignment with ISO 27001:2022 control measures, including "A.5.30 ICT Readiness for Business Continuity," "A.8.9 Configuration Management," and "A.8.16 Monitoring Activities." The aim is to validate the feasibility of the mitigation plan, serving as a recommendation for the development of information security technologies for 6G network software and hardware.

C. During the information security seminar in this project, the majority of industry participants expressed concerns about the increasing security threats as the deployment of 5G dedicated networks continues to rise. They recommended that government agencies study the extension of 5G to 6G and establish relevant information security standards and regulations. These standards should be based on those published by multilateral organizations and advanced international countries. Alternatively, the government could consider the SOP mechanism for 6G security scenarios and promotional procedures. This step-by-step approach aims to develop a communication network security management system, ensuring the resilience and security of the communication environment in Taiwan. Such efforts will benefit Taiwanese industry players in gaining access to the international 6G supply chain.

D. In consideration of the international trends in communication security and the technical focus of this project, we conducted four technical exchange seminars. These seminars hosted over 50 participants from various sectors, including dedicated network operators, system integrators, equipment suppliers, security experts, and research institutions. The goal was to gather perspectives on security themes within different communication generations, which will serve as a reference for the development of a secure foundation for 6G service architectures.

(5) Pre-6G Inter-ministerial Cooperation Working Group

A. Three conferences of the Pre-6G Inter-ministerial Cooperation Working Group have been successfully conducted. During these conferences, participants from the MOEA of the



- Ministry of Economic Affairs, IDA of the Ministry of Economic Affairs, and NTSC gathered to discuss and coordinate various aspects related to the advancement of 6G, with the aim of fostering 6G development in the country.
- B. Completed three cases of supporting government or telecommunications industry participation in international organizations related to 6G applications and standards. These efforts have aimed at fostering international cooperation, exchanges, and engagement in significant global events by harnessing the combined efforts of various ministries and bridging the public and private sectors.
- C. Published 9 e-newsletter, consolidating information on domestic and international MICE events. This information is made available to industry, government, and academia to facilitate pre-event networking and to provide the latest updates on international telecommunications, promoting resource sharing.
- D. Established three information collaboration platforms, which include providing team members with a channel for pre-application communication regarding experimental frequencies, conducting surveys for participation in the 2023 and 2024 international conferences, and facilitating communication for planning and collaboration in the organization of the 2024 international conference.

4. Following-up

(1) Immediate recommendations

- A. The existing outcomes of this project can be provided to the TAICS (Taiwan Association of Information and Communication Standards) for 6G cross-disciplinary application associations, serving as reference cases for

preliminary planning or proposing recommended standards. For instance, relevant committees within TAICS, such as TC1 (Advanced Mobile Communication), TC3 (Device Networking Working Group), and TC-5 (Networking and Information Security Working Group), will regularly share the results of this project's content. Additionally, they will provide suggestions or propose standards in alignment with international standard trends as needed.

B.By leveraging Cloud-Native combined with generative AI technology in communication-related application domains, as well as employing Distributed Ledger Technology (DLT) for applications based on data privacy, we aim to collaborate with relevant alliance/association partners, such as the MIH Consortium and Taiwan Association for Blockchain Ecosystem Innovation. Our goal is to propose directions for technologies and applications that align with the 6G and 9G trends in the future. Through active engagement, we will exchange ideas, suggestions, and explore collaboration opportunities with alliance and association members, utilizing the collective R&D resources of this project to jointly establish a preliminary proof of concept.

C.Coordinate the aforementioned efforts and information sharing within the Public Sector Linkage Group, offering them as references or fostering collaboration for other sub-groups. Additionally, plan to invite exceptional scholars, experts, and innovators both domestically and internationally to engage in discussions within the Pre-6G Inter-ministerial Cooperation Working Group.

D.The outcomes of this project, including recommendations and practical cases related to information security in the Structured

Threat Information eXpression (STIX) framework, potential attacks when introducing AI applications into the nuclear network, and empirical results from cross-disciplinary AI applications, will be utilized to facilitate exchanges between the Department of Resource Management at the Ministry of Digital Affairs and relevant entities, such as the NICS, NCC, and others. Furthermore, the results of this project will be used to provide insights or advocate for the implementation of recommendations to the overseeing authorities.

(2)Mid and Long-term Proposals

- A.Drawing inspiration from the advancements in FIDO-integrated communication applications and the ongoing development of post-quantum cryptographic enhancements, we aim to strategically plan the integration of cross-disciplinary applications involving AI, hybrid networks, and 6G communication features. This integration will be designed with robust information security and privacy protection mechanisms, propelling the industry to proactively deploy 6G application technologies ahead of schedule."
- B.Continuously monitor future developments in AI regulations and security from the European Union, the United States, and international and standards organizations. Building upon the trends and practices in promoting trustworthy AI, this project will integrate AI applications with features such as security, privacy, and resilience. The plan includes proposing technology development and validation with a focus on Distributed Ledger Technology (DLT), AI applications/security, and Federated Learning (FL) as the primary axes.



C. Actively participate in cross-disciplinary 6G application associations, serving as reference cases for preliminary planning and proposing specifications. Examples include the TC3-Device Networking Working Group and TC-5 Networking and Information Security Working Group within the TAICS. Regularly share the outcomes of this project with these associations and, as needed, put forth recommendations or proposals aligning with international standard trends.

第一章 緒論

第一節 計畫背景

第六代行動通訊(The 6th Generation Wireless Systems, 6G)，按照過往行動通訊技術約每 10 年會更新一代的演進歷程，預估在 2030 年 6G 將可實現商用化。

雖然目前第三代合作夥伴計畫(3rd Generation Partnership Project, 3GPP)尚未啟動有關 6G 規格的研制工作，然而目前根據各國、各大廠商所闡述的 6G 願景，可以比較明確預期未來 6G 基礎建設運作環境的特徵將涉及超高速(Extreme High Data Rate)、超覆蓋(Extreme Coverage)、超節能(Extreme Low Energy)、超低延遲(Extreme Low Latency)、超信賴(Extreme High Reliability)、超連結(Extreme Massive Connectivity)等。

架構於上述的 6G 基礎建設願景下，各廠商、機構所思考的跨領域應用服務有各種差異，譬如多感官的延展實境(Extended Reality, XR)、聯網機器人和自主系統、智慧工廠、數位孿生等應用。但是，探索應用服務底層的技術基礎主要涉及到資訊安全、人工智慧(Artificial Intelligence, AI)及感知資訊應用 3 個面向的技術，而且有別以往是以外加的模式附加於應用服務上，有些單位發布的白皮書，是建議將 AI 及資訊安全高度內嵌在 6G 行動網路基礎建設中。

以下就此 3 個技術議題進行比較深入的探討：

一、資訊安全是應用服務成功的重要關鍵

資訊安全除一般所謂的網路安全、資料保護等傳統資安議題外，因為未來的應用服務會保存很多使用者個資，目前應擴及至所謂個人隱私資訊保護功能，不管是在那個環境，資訊安全、隱私保護等議題都應該是所有應用服務的必要考量。未來在 6G 行動網路的環境下，預期可達到無縫立體的全域覆蓋連接。於此基礎下，會有萬物互聯的



情況出現。這意味著將會有更多的人、物、服務連上網路，就有更多資料甚至是隱私個資會在網上到處傳遞，所以資訊安全的防護也就越顯得重要。

二、AI 是眾多應用服務的基礎

6G 的智慧化應該是貫穿網路端到端的每一個環節，有些機構規劃蒐集網路流量的資料，運用 AI 內嵌於 6G 行動網路系統中，優化網路運作效能；或使用 AI 技術分析大量產生的資料，輸出分析結果給予判斷，並進行後續適當處理。

三、感知資訊異質網路傳遞應用

目前大部分機構對 6G 發展推估，預計在 2030 年會達到一定程度，認為當時的特徵之一，是資料將會驅動社會上產生更多的應用。感知能力將是行動通訊系統在 6G 時代基本通訊能力之外的一大重要能力，日本甚至認為會是一個「資料驅動型社會」。為實現這一轉變，將使用各種感知器收集眾多的最新資料，接收網路世界上各種感知資訊，了解發生在海洋、天空、甚至外太空等實體空間中的各種現象。

面對未來 6G 跨領域應用趨勢，考量善用政府珍貴資源。將於本年度的計畫規劃上，思考如何建立安全且可靠的機制，提供跨領域應用可被民眾信任的基礎，及分析 AI 應用到 6G 整體系統中那些對於應用可靠性、安全性以及隱私保護需求中適當且迫切的部分。

第二節 計畫架構

為布局我國 6G 自主技術能量，使臺灣成為全球主流系統重要策略夥伴。本計畫將先期投入 6G 產業發展規劃相關重要工作，除了通訊系統之外，相關的數位科技應用技術、標準、智財也是兵家必爭之地。其中又以 AI、資安隱私 2 項數位科技應用最為關鍵，故將以涵蓋應用端以應用情境導向整合 AI 應用與 6G 通訊特性，以及資安與隱私防護的需求，對未來 6G 商轉可能遭遇的問題與技術需求進行規劃與初期驗證。此外，將持續維運公部門連結小組，針對 6G 發展各項議題，進行跨部會協商與意見整合。

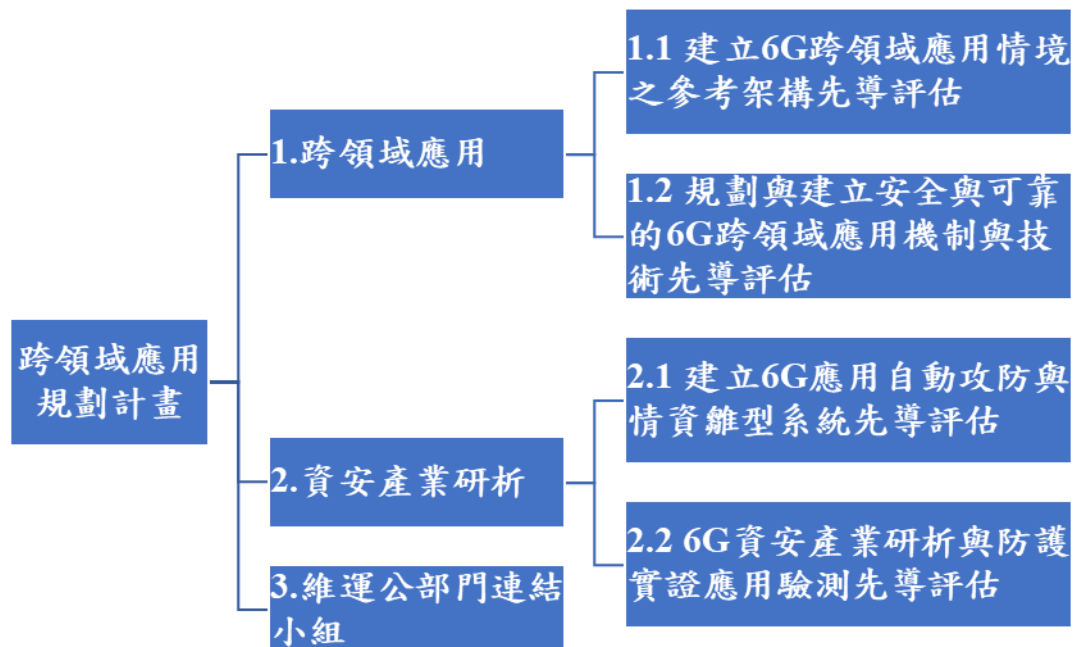


圖 1、計畫架構圖

資料來源：本計畫整理

第三節 計畫執行內容

本計畫共包含「跨領域應用」、「資安產業研析」、「維運公部門連結小組」3 項主題，以下分別敘述各主題工作內容：

一、跨領域應用

此主題包含「建立 6G 跨領域應用情境之參考架構先導評估」及「規劃與建立安全與可靠的 6G 跨領域應用機制與技術先導評估」2 工作項，以下就各項工作項進行說明：

(一)為完成本委託案日常業務支援工作之推動，廠商至少應派駐 2 名人員，相關工作項目成果如附件 1。

(二)建立 6G 跨領域應用情境之參考架構先導評估

1. 蒐集研析 AI 原生(AI-Native)6G 及雲端原生(Cloud-Native)6G 之跨領域應用情境參考架構

應包括但不限於協同分析應用之低延遲設計與通訊效率強化及具備大量裝置共同協作與動態加入/退機制，如模型剪枝、梯度壓縮等。

2. 持續追蹤 6G 應用標準趨勢與進程。
3. 研擬與驗證跨應用層與網路層通訊強化機制。
4. 完成跨領域應用情境實證與離型系統先導評估。

(三)規劃與建立安全與可靠的 6G 跨領域應用機制與技術先導評估

1. 發展容錯技術強化服務韌性

可不受網路層或裝置端發生錯誤或失效而導致服務的不穩定。

2. 分散式服務架構或大量裝置情境分析層面的安全議題

基於該情境下，如惡意資料攻擊、資料竊取、模型攻擊等議題。

3. 完成跨領域應用情境的安全與可靠實證先導評估。

二、資安產業研析

此主題包含「建立 6G 應用自動攻防與情資離型系統先導評估」及「6G 資安產業研析與防護實證應用驗測先導評估」2 工作項，以下就各項工作項進行說明：

(一)建立 6G 應用自動攻防與情資離型系統先導評估

1. 6G 應用服務層之偵防工具化可行性評估

就 6G 訊設備及服務至少 5 種威脅項目進行技術先導評估，如 AI 原生安全性(AI-Native Security)、in-X 子網 Network Slicing Security、IP 欺騙(IP Spoofing)、阻斷服務攻擊(Denial of Service, DoS)、降級攻擊(Downgrade Attack)及資料外洩等。

2. 研析潛在 6G 標準技術之相關滲透測試規範

可支援 6G 網路威脅訊結構，如網路威脅情資結構化資料交換格式(Structured Threat Information eXpression, STIX)。

3. 完成 6G 應用自動攻防與情資離型系統實證先導評估：

須明確說明與 ISO 27001 控制項目之對應及改善成效。

(二)6G 資安產業研析與防護實證應用驗測先導評估

1. 未來 6G 資安服務框架、對應防護情境與推動程序 SOP 機制

訪談業者對於資安服務框架、防護情境與推動機制，並推動業者參與未來場域中可能用營運之狀況與對應推動機制。

2. 完成 6G 資安產業研析與防護實證先導評估

須明確說明與 ISO 27001 控制項目之對應及改善成效。



3. 座談會辦理

參酌國際發展經驗及蒐集資料，辦理座談會 4 場次，邀請討論議題之相關利還關係者，蒐集國內現況及產官學等意見。

三、維運公部門連結小組

(一)辦理公部門連結小組會議

持續運作 111 年已成立之公部門連結小組，每季應至少辦理 1 場次公部門連結小組會議，並彙整各部會進度資料於公部門連結小組會議中報告。

(二)協助國際標準組織參與及建立國際合作管道/案例。

(三)觀測國際應用服務展及國內產業能量盤點

點出 6G 應用服務技術及資安發展策略，提供政府決策參考。

第四節 6G 關鍵技術指標

一、6G 關鍵性需求 KPI

依 FY111 跨領域應用規劃計畫，彙整各國際組織、企業之報告及白皮書，其對 6G 相關的關鍵性技術指標共包含傳輸延遲(Latency)、定位精準度(Positioning accuracy)、覆蓋範圍(Coverage)及用戶端/設備連接密度(Connection density)等。詳細各單位對 6G 關鍵技術指標如表 1：

表 1、6G 關鍵性需求 KPI

KPI	說明	需求(v.s. 5G)
峰值傳輸速率 (Peak data rate)	每個用戶或設備在理想條件下可達到的最大數據速率，以 Gbit/s 表示	1 Tbit/s (20 Gbit/s)
用戶體驗數據速率 (User – experienced data rate)	使用者有至少 95%的機率可以在任何時間或地點獲得此數據速率，以 Mbit/s 或 Gbit/s 表示	1 Gbit/s (100 Mbit/s)
傳輸延遲 (Latency)	從來源端發送一個數據封包至目的端接收所需的時間，以 ms 表示	0.1 ms (1 ms)
移動性 (Mobility)	在屬於不同的傳輸層和無線接取技術 (Multi-layer/Radio Access Technology, RAT) 的無線節點間在被限定傳送服務品質 (Quality of Service, QoS) 與無縫轉移下，可以實現的最快速度 (以 km/h 表示)	1000 km/h (500 km/h)



KPI	說明	需求(v.s. 5G)
用戶端/設備連接密度 (Connection density)	每單位面積的設備連接數和進行通道存取的總數，以 km^2 表示	$107/\text{km}^2$ ($106/\text{km}^2$)
能源效率 (Energy Efficiency)	網路端：從用戶接收或傳送過程中，每單位無線接取網路 (Radio Access Network, RAN) 的能量消耗所能傳遞位元的數量 (以 bit/Joule 表示) 設備端：每單位通訊模組能量消耗所能傳遞的位元數量 (以 bit/Joule 表示)	1Tbit/Joule (比 5G 降低 10 – 100 倍)
頻譜使用效率 (Spectral efficiency)	每單位的頻譜資源與單位蜂巢細胞涵蓋範圍的平均數據傳輸量，以 bit/s/Hz 表示	60 bit/s/Hz (比 5G 提高至少 3 倍)
區域傳輸流量 (Area traffic capacity)	每單位區域的數據服務總流量，以 Mbit/s/ m^2 表示	1Gbit/s/ m^2 (100 Mbit/s/ m^2)
可靠性 (Reliability)	在 1ms 內成功傳送 32 bytes 的機率，以 % 表示	99.99999% (99.999%)
訊號頻寬 (Signal bandwidth)	Radio frequency 頻寬，以 bit/s/Hz 表示	1 GHz (100 MHz)
定位精準度 (Positioning accuracy)	定位的精準程度，以 m 表示誤差	0.01 m (1 m)
覆蓋範圍 (Coverage)	網路的覆蓋範圍	3D 地面-衛星-空中的整合網路系統 (僅 2D 地面網路)

KPI	說明	需求(v.s. 5G)
時效性 (Timeliness)	強調訊息新鮮度的衡量指標 (AoI/T/S, Information/Task/synchroniza- tion)，對於要求時效性的應用 (如自動駕駛)極重要	N/A
安全與隱私 (Security and privacy)	為滿足大量的萬物聯網 (Internet of Everything, IoE) 設備連線，及在不受信任的環 境中部署衛星-無人機以建立 物聯網 (Internet of Things, IoT)通訊，皆需發展能保證資 料不外洩的新技術	N/A

資料來源：本計畫整理

二、本計畫對應關鍵性 KPI

本計畫進一步針對 6G 技術需求指標，對應在跨領域應用服務上的情境與需求，逐步探討可能的技術選項並進行評估與技術實證。本計畫對應 6G 關鍵性技術指標包含傳輸延遲(Latency)、用戶端/設備連接密度(Connection density)、可靠性(Reliability)及安全與隱私(Security and privacy)，詳細對應關鍵性技術指標如表 2：

表 2、6G 關鍵性技術指標對應表

(一)建立 6G 跨領域應用情境之參考架構先導評估	
對應 6G 關鍵性技術指標	說明
- 用戶端/設備連接密度 (Connection density) - 安全與隱私 (Security and privacy)	允許大量且密集的使用者參與，豐富的資料將提高模型正確率；伺服器不保留資料，使用者上傳訓練完即丟棄或只上傳權重，除確保隱私外，也不影響辨識正確率（可辨識新/舊類別）。

(二) 規劃與建立安全與可靠的 6G 跨領域應用機制與技術先導評估

對應 6G 關鍵性技術指標	說明
- 傳輸延遲(Latency) - 可靠性(Reliability) - 安全與隱私 (Security and privacy)	資料就近於邊緣處理，減少封包延遲，並以區塊鏈(Blockchain, BC)、分散式帳本技術分散式系統方式實作資料複製及系統，建立 IoT 去中心化服務實驗架構，維護網路的可信任性，滿足零信任(ZeroTrust, ZT)原則。

(三) 建立 6G 應用自動攻防與情資離型系統先導評估

對應 6G 關鍵性技術指標	說明
- 可靠性(Reliability) - 安全與隱私 (Security and privacy)	識別出網路攻擊，防止資料洩漏、未經授權存取、產生潛在風險、導致資安及隱私問題，並且減緩阻斷資源而發生網路中斷、資源消耗，影響關鍵基礎設施導致系統無法正常運行，降低系統可信賴性。

(四) 6G 資安產業研析與防護實證應用驗測先導評估

對應 6G 關鍵性技術指標	說明
- 可靠性(Reliability) - 安全與隱私 (Security and privacy)	基於對 6G 無線網路基礎架構元件的特性，避免使用者認證資訊產生洩漏風險，阻斷使用者應用無線網路服務，並防止偽冒網路基地臺，避免攻擊者誘騙網路用者，導致隱私資訊洩漏，降低系統可信賴性。

資料來源：本計畫整理

第五節 研究方法

一、本計畫研究方法

(一)文獻分析法

文獻分析法是指根據一定的研究目的或課題，透過蒐集有關市場資訊、調查報告、產業動態等文獻資料，從而全面且精準地掌握所要研究問題的一種方法。蒐集內容儘量要求豐富及廣博，再將四處收集來的資料，經過分析後歸納統整，再分析事件淵源、原因、背景、影響及其意義等。文獻資料可以是政府部門的報告、工商業界的研究、文件記錄資料庫、企業組織資料、圖書館中的書籍、論文與期刊、報章新聞等。其分析 4 步驟包含閱覽與整理、描述、分類及詮釋。^{1.1}

(二)訪談法

訪談法用於理解受訪者對研究問題的看法，或陳述對生活、經驗或情況的觀點等所採用的方法。研究者以觀察者和參與者的身分，記錄與研究對象或研究對象間言談互動，並由對話過程發現人們對社會事實的認知，或分享經驗與觀點的互動方式。訪談法不同於日常生活的交談，具有一定目的和形式。訪談者與受訪者雙方的地位和權力可能不一樣，是一種人為的談話環境。交談的內容、談話的風格以及資訊的類型與多寡，都可能和日常生活的交談不同。

(三)實驗法

實驗法是在控制環境中，研究者有計畫性地操控實驗變數，觀察或測量此操控對實驗結果的影響之研究程序。在控制環境中進行實驗法的意義是要盡可能排除實驗變數外，其他會對研究結果產生影響的因素(變數)。因此，執行實驗法的主要目的，期望單純的觀

1.1 W. Lawrence Neuman 著朱柔若譯. 社會研究方法－質化與量化取向(2000)

察測量或測量實驗變數對實驗結果的影響，以解析實驗變數和實驗結果之間的因果關係。

二、各工作項計畫執行方式

依據不同工作內容，採用適當之研究訪法，以下就各項工作內容依照執行面需求，分別說明工作分項的研究方法，及執行方式：

(一)建立 6G 跨領域應用情境之參考架構先導評估

本分項計畫採用文獻分析法蒐整 AI-Native 6G 和 Cloud-Native 6G 之跨領域應用參考情境，以探索未來 6G 網路應用的發展趨勢與標準進程。

首先本計畫將說明建立 6G 跨領域應用情境的必要性和重要性，包括對 6G 網路的特點與優勢的闡述，並著重強調 6G 技術在不同應用領域的潛在價值。接著探討 6G 應用的趨勢、發展情境以及願景與 IMT-2030 發展架構，將成為建立跨領域應用情境參考架構的基礎，有助於確定 6G 技術在未來的應用方向和發展脈絡；透過深入瞭解 6G 應用的現狀和未來，能更了解參考架構的定位和目標。

藉由蒐集研析 AI-Native 6G 和 Cloud-Native 6G 之跨領域應用情境參考架構，探討 2 種架構在不同應用場景下的運作和特徵，以及對於 6G 技術跨領域應用的影響和優勢。同時也會詳細分析跨應用層和網路層的通訊強化機制，整理有助於模擬研究的適當開源軟體，用以提高 6G 網路在跨領域應用中的表現，為參考架構建立提供實質性依據。

在實證階段，本計畫建立跨領域應用雛型系統的基礎環境設定，並詳細說明實證效果。藉此驗證所建立參考架構的可行性與效能，並為未來 6G 網路應用實現提供指引。本分項將實作類別增量學習 (Class-Incremental Learning, CIL) 技術，驗證符合 6G 的 Connection density 及 Security and privacy 技術指標，並在智慧商店商品辨識新

增類別的跨領域應用情境下，實作 CIL 與傳統機器學習演算法比較正確率，實證滿足現實世界中跨領域應用需求。

(二)規劃與建立安全與可靠的 6G 跨領域應用機制與技術先導評估

本分項研究方法採取文獻分析法探討 B5G/6G 去中心化服務架構技術，範圍包括次世代網路(Next Generation Networks, NGN)及物聯網(Internet of Things, IoT)裝置等去中心化服務相關論文及國際標準。搜尋的參考文獻來自於 IEEE Xplore、ScienceDirect 等資料庫，國際標準則涵蓋歐洲電信標準協會(European Telecommunications Standards Institute, ETSI)、國際電信聯合會(International Telecommunication Union, ITU)、國際標準化組織(International Organization for Standardization, ISO)及電機電子工程師學會(Institute of Electrical and Electronics Engineers, IEEE)等組織所訂定的標準。同時也透過相關開源軟體發布的訊息進行研究分析，提出對應安全與可靠的 6G 跨領域應用機制與技術之建議。

經文獻收集、分析，並與各國際大廠發布之訊息比對後，發現各國際標準組織自 2017 年起，陸續以分散式帳本技術(Distributed Ledger Technology, DLT)為基礎訂定去中心化服務架構標準，用於包括自駕車或工廠自動化(需大量 IoT 設備)等應用之資料分享。

其中 DLT 用於建立零信任(ZeroTrust, ZT)，即是不假設任何用戶和系統是可信的跨領域安全環境，使得各種資料可在 6G 網路中安全分享，並進一步用於機器學習(Machine Learning, ML)與 AI 來達成資料驅動決策的最終目標。此外，目前也有許多論文及開源計畫使用 DLT 技術，在 B5G/6G 環境中建立分散式儲存系統，以避免單點失敗增加系統容錯能力。因此，本分項依此趨勢於安全與可靠的 6G 跨領域應用機制先導評估項目中，建立去中心化資料分享實驗平臺。將應用情境設定為 IoT，同時提供平臺資料安全、隱私保護及系統容錯等能力，為 6G 跨領域安全環境之鋪設踏出第一步。

(三)建立 6G 應用自動攻防與情資雛型系統先導評估

本分項採用文獻分析、比較法，並與領域技術專家合作。茲分別說明如下。首先，探索產學研領域對於主要資安威脅(DoS、IP Spoofing、Downgrade Attack、Network Slicing、AI-Native)在 B5G/Pre-6G 階段的最新研究文獻。期望從中整理分析出對於未來 6G 網路層、服務層、應用層等資安威脅可能發動的攻擊、如何進行偵測與防禦、如何緩解攻擊。此外，本計畫也關注這些攻擊分別對於 5G 與 6G 通訊架構的差異比較。由於 6G 標準尚未定義，因此針對 6G 資安議題前期研究，最有效方法便是整理相關領域最新研究成果，從研究者角度來探索問題，並藉由不同研究者的比較分析，歸納出較具共識的結論。

此外，也和領域學者、技術專家進行合作，以幫助本計畫進行實測驗證，能夠具體安排可行的驗證情境。例如在 5G 與 6G 都缺乏 AI-Native 網路元件，技術專家建議透過開源軟體、數值模擬可以解決目前 5G 通訊環境尚不支援的問題。透過技術專家的見解和經驗，讓本團隊能夠預見可能的挑戰，並相應調整實測驗證，根據其建議使用開源模擬工具來建構 5G 和 6G 網路元件模擬環境，儘管存在技術限制，仍可確保實驗的有效性。

(四)6G 資安產業研析與防護實證應用驗測先導評估

本分項研究方法將採取文獻分析法、政策與市場參與者訪談，探討國際先進國家及多邊組織等發展 B5G/Pre-6G 關鍵技術、商用市場與資安應用之動態發展趨勢。儘管技術研究和系統工程在探索 6G 細節仍處於早期階段，然產業共識是圍繞關鍵技術前提形成的，本團隊將搜尋參考文獻，如 IEEE Xplore、全球科技研究及顧問機構(ISG Research)、國際資料資訊有限公司(International Data Corporation, IDC)或國際顧能有限公司(Gartner)等。此外透過各國

際大廠業者之新聞發布動態輔以進行研究分析，提出對應 6G 應用情境之資安服務框架與推動建議。

資料蒐集分析後，進行文獻的論述及國內通訊產業現況做比較，盡可能掌握如 3GPP、ITU、美國國家標準暨技術研究院(National Institute of Standards and Technology, NIST)、歐盟網路安全局(European Union Agency for Cybersecurity, ENISA)等國際組織初探 6G 應用場景。制訂全球通訊標準之進程至 2024 年可視為 6G 技術的前緣，採用 6G 開放式無線接取網路(Open Radio Access Network, O-RAN)系統架構，提出 6G 核心網路以及 O-RAN 介面遭受到攻擊的樣態及影響，關注通訊安全主題和 O-RAN 架構推動的分解，可能帶來的各種挑戰，建議對應資安防護應用與導入機制，為構築 6G 世代的網路安全技術融合奠定基礎。

其中一環參考 3GPP 最新審議中 Release-18(R18)技術標準，於測試模擬器上搭建 LTE/Pre-6G 環境，模擬針對入網設備身分驗證程序探究安全問題，可能導致駭客可控制或崩潰整個通訊網路，進而建議緩解措施或提案增修國際通訊安全標準。

第六節 預期成果

依照本計畫各主題，包含跨領域應用、資安產業研析、維運公部門連結小組，其預期產出成果說明：

一、跨領域應用

- (一)在跨領域應用情境的研究上，規劃蒐集 AI-Native 6G 及 Cloud-Native 6G 之跨領域應用情境參考架構，透過上述情境研析推展可供參考的應用領域。並探討可能的需求與技術方案，透過實證驗證其可行性，以做為未來研發 6G 跨領域應用服務系統之依據。
- (二)未來 6G 跨領域應用情境，必然將行動網路與客戶資料整合，行動網路需要一個安全可靠與受信賴的分散式運算環境，允許在沒有預先建立信任關係的各方共享資料，以滿足 AI 技術需要大量訓練資料。另一方面也可保護用戶通訊的安全及隱私，本計畫預計研究以聯合學習(Federated Learning, FL)、ZT 架構、區塊鏈(Blockchain, BC)等，以滿足跨領域應用情境下的需求與挑戰。並透過實證建構一個環境，來達成前述目的並進行探討與評估。
- (三)持續追蹤各 6G 聯盟如 Next G Alliance、Hexa-X 以及標準/類標準組織，如 ITU、ISO、3GPP 與開放工程聯盟(MLCommons)等，對未來 6G 應用服務的情境展開與技術架構，滾動修正本計畫之規劃與發展方向，以期在 6G 正式推進時，協助國內產業發展相關技術與產品服務。

二、資安產業研析

- (一)提早布局 6G 資安威脅的偵防技術研發，協助國內產業界累積相關研發能量，及早面對與規劃 6G 資安威脅下的對應策略，建構出創新、前瞻、國際性的視野。

(二)研析最新的國際標準，如 ISO 27001:2022、STIX v2.1，有利於未來落實 6G 資安整體防護。透過 STIX v2.1 所建構的資安威脅情資描述共通格式，引導國內產業界建立協作機制。並與國際接軌、分享、獲取最新資安威脅情資，讓 6G 環境安全保護更加提升。

(三)6G 世代的發展，將會快速衍生產業典範移轉，例如衛星通訊可能取代現行衛星新聞轉播(Satellite News Gathering, SNG)車輛通訊，未來新聞電視臺將成為 6G 整體生態中的一環，而不再是自成一套與行動通訊無關的通訊體制。因此 6G 網路資安防護也將具有生態特性，透過本計畫先期 6G 資安產業研析與防護實證，以及辦理產業座談會交流，將能協助產業界提供 easy-to-use 解決方案，促進業者在資安議題上無縫接軌地強化供應鏈/關係企業/跨國公司等合作協同關係。同時滿足聯合國永續發展目標(Sustainable Development Goals, SDGs)，建立下世代行動通訊之國家級數位韌性及數位自主的信任產業。

三、維運公部門連結小組

作為跨部會溝通平臺，協調推動 6G 發展相關議題，有效掌握國際趨勢。並透過規劃資源協作平臺，讓公部門相關計畫間的資訊更為通透，整合國內能量，一起參與國際盛會，進而帶動新興應用服務及系統整合發展。

第七節 計畫執行狀況

一、目標達成狀況

依照計畫內容之工作項目，各項目下另外劃分為數個執行細項，目前計畫依照原先規劃應於 112 年度計畫開始日至期末審查日完成之各工作進度執行，各工作執行進度如表 3 所示：

表 3、計畫進度甘特圖

執行進度 \ 月份	2	3	4	5	6	7	8	9	10	11	12
一、跨領域應用規劃											
(一)建立 6G 跨領域應用情境之參考架構先導評估											
蒐集研析 AI-Native 6G 之跨領域應用情境參考架構											
蒐集研析 Cloud-Native 6G 之跨領域應用情境參考架構											
持續追蹤 6G 應用標準趨勢與進程											
研擬與驗證跨應用層與網路層通訊強化機制											
完成跨領域應用情境實證與雛型系統先導評估											
(二)規劃與建立安全與可靠的 6G 跨領域應用機制與技術先導評估											
發展容錯技術強化服務韌性											



月份	2	3	4	5	6	7	8	9	10	11	12
執行進度											
分散式服務架構或大量裝置情境分析層面的安全議題											
完成跨領域應用情境的安全與可靠實證先導評估											
二、資安產業研析											
(一)建立 6G 應用自動攻防與情資離型系統先導評估											
6G 應用服務層之偵防工具化可行性評估											
研析潛在 6G 標準技術之相關滲透測試規範											
完成 6G 應用自動攻防與情資離型系統實證先導評估											
(二)6G 資安產業研析與防護實證應用驗測先導評估											
未來 6G 資安服務框架、對應防護情境與推動程序 SOP 機制											
完成 6G 資安產業研析與防護實證先導評估											
座談會辦理											
三、維運公部門連結小組											
辦理公部門連結小組會議											



月份	2	3	4	5	6	7	8	9	10	11	12
執行進度											
協助國際標準組織參與及建立國際合作管道/案例											
觀測國際應用服務展及國內產業能量盤點											
期中報告提交	112 年 7 月 12 日										
期末報告提交	112 年 11 月 1 日										

資料來源：本計畫整理

二、目標執行成果

本計畫執行各分項工作如表 3 所列，期中及期末產出之報告及其質化內容如表 4 所列：

表 4、期中期末工作量化指標與質化產出

期中期末進度 工作項目	期中報告產出	期末報告產出
一、跨領域應用規劃		
(一)建立 6G 跨領域應用情境之參考架構先導評估		
蒐集研析 Cloud-Native 6G 之跨領域應用情境參考架構	Cloud-Native 6G 之參考架構研析及服務面向報告 研析 Cloud-Native 的重要特徵、目前市場應用狀態以及技術發展趨勢，並整理其優缺點。	Cloud-Native 6G 之參考架構研析及服務面向報告 研析虛擬化的應用及發展趨勢，蒐集、整理各種解決方案，完成對應用服務的技術適用性分析。
蒐集研析 AI-Native 6G 之跨領域應用情境參考架構	AI-Native 6G 之參考架構研析及服務面向報告	AI-Native 6G 之參考架構研析及服務面向報告



期中期末進度 工作項目	期中報告產出	期末報告產出
	蒐集、研析國際上對於 AI-Native 討論，整理出未來 AI-Native 在未來 6G 行動通訊環境下的特徵。	探索 AI-Native 的研究意見，解析未來應用服務與 AI-Native 互動關係，建議不同性質的服務，應考量的網路特徵。
持續追蹤 6G 應用標準趨勢與進程	國際 6G 應用標準趨勢及進程蒐集報告	國際 6G 應用標準趨勢及進程蒐集報告
	研析 ITU-R 對 IMT-2030 的 6G 趨勢及未來情境說明。	研析國際組織及電信商的 6G 趨勢及未來情境說明。
研擬與驗證跨應用層與網路層通訊強化機制	跨應用層與網路層通訊強化機制研析報告	跨應用層與網路層通訊強化機制實證報告
	1. 通訊強化機制研究：探討在 6G 通訊領域的應用，如何提升應用層和網路層之間的通訊效能 2. 開源軟體調研：整理 4 種常用的開源軟體以及應用場景，並分析這些開源軟體的局限性	探索目前 6G 以及跨應用層和網路層通訊強化機制相關的研究主題和技術，例如多連接技術、增強現實和虛擬現實通訊、網路安全和隱私、人工智慧的應用、綠色通訊等。
完成跨領域應用情境實證與雛型系統先導評估	跨領域應用情境實證及雛形系統研析報告	跨領域應用情境實證及雛形系統先導評估報告
	聯合新增類別學習方法研究。	以智慧手機為測試平臺實作 6G 跨領域應用



期中期末進度 工作項目	期中報告產出	期末報告產出
		情境，並產出分析報告。
(二)規劃與建立安全與可靠的 6G 跨領域應用機制與技術先導評估		
發展容錯技術強化服務韌性	容錯技術研析報告	容錯技術強化服務韌性發展研析
	完成邊緣運算環境建構去中心化管理機制及分散式系統可行性研析。	研析虛擬化網路元件的監督技術以加強系統容錯能力。
分散式服務架構或大量裝置情境分析層面的安全議題	分散式服務架構或大量裝置情境研析報告	分散式服務架構或大量裝置情境實證報告
	研析 BC 結合 IPFS 部署於邊緣運算環境並用於 IoT 應用之可行性。	研析 IPFS 擴展功能以及架設私有 IPFS 網路之可行性。
跨領域應用情境的安全與可靠實證先導評估	評估各開源邊緣運算之完成度	完成跨領域應用情境的安全與可靠實證先導評估報告
		以開源邊緣運算環境為測試平臺，建立 BC 及 IPFS 叢集，並使用 IoT 模擬器測試效能。同時也會架設虛擬化網路元件的監督平臺，評估容錯能力。



期中期末進度 工作項目	期中報告產出	期末報告產出
二、資安產業研析		
(一)建立 6G 應用自動攻防與情資離型系統先導評估		
6G 應用服務層之偵防工具化可行性評估	6G 應用服務層之偵防工具化可行性評估報告	6G 應用服務層之偵防工具化可行性評估報告
	完成 5 項威脅的研析，說明在 5G 環境下作用的原理、攻擊方法、防禦方法、以及相關偵防工具。對於 6G 時代的如何應對同類威脅，可以做為重要的參考依據。	對於偵防工具的研析，將持續更新目前國際上的最新發展進度。
研析潛在 6G 標準技術之相關滲透測試規範	6G 標準技術之相關滲透測試規範研析報告	6G 標準技術之相關滲透測試規範實證報告
	完成滲透測試規範與 STIX 規範的研析。可做為對未來 IoT 進行滲透測試的指引。	對於相關規範的研析，將持續更新目前國際上的最新發展進度。
完成 6G 應用自動攻防與情資離型系統實證先導評估	6G 應用自動攻防與情資離型系統研析規劃。	6G 應用自動攻防與情資離型系統實證先導評估報告
		驗證 6G 無線資源配置 AI 模型功能遭受傳統攻擊，以及 AI-Native Security 的攻擊方式、



期中期末進度 工作項目	期中報告產出	期末報告產出
		影響及防禦策略，可以強化 RAN 及其服務安全的認識，觀察 RAN 服務品質受到攻擊影響的程度與範圍，收集資料作為調整防護策略的依據。
(二)6G 資安產業研析與防護實證應用驗測先導評估		
未來 6G 資安服務框架、對應防護情境與推動程序 SOP 機制	6G 資安服務框架、對應防護情境與推動程序 SOP 訪談及研析報告	6G 資安服務框架、對應防護情境與推動程序 SOP 研析報告
	針對 RAN 在 R18 標準中，著重行動、負載平衡和節能作用，R19 標準中對於 6G 的討論，提供國際上討論 6G 前瞻技術的挑戰中，網路安全是未來部署中需要重視的關鍵環節。	由國際 6G 資安技術與市場發展動態，分析我國通訊產業 6G 環境發展現況，探討發展通訊資安產業面臨之挑戰與機會，提出 6G 應用情境之資安服務框架建議方向。
完成 6G 資安產業研析與防護實證先導評估	依據座談會意見以及產業研析，分析未來 6G 產業需求。	6G 資安產業研析與防護實證先導評估報告
		發展 2 大類型 4 種資安攻擊情境，測試攻擊發生的影響程度，技術實證結果對應 6G 關鍵性技術指標可靠性與安



期中期末進度 工作項目	期中報告產出	期末報告產出
		全和隱私，在國內廠商參與國際組織討論會議時，回饋國內 Pre-6G 相關資安技術的前期研究與測試結果，形成國內外技術同步的正向循環。
座談會辦理	辦理資安座談會共計 1 場次	辦理資安座談會共計 4 場次
	112/5/16「支援零信任(ZT)架構的定期評估」座談會。	1.112/8/29「用 AI 感知世界 以資安防護未來」座談會 2.112/9/19「從 5G 到 6G 邊緣運算資安變革與商機」座談會 3.112/10/5「萬物皆可駭，5G/6G 物聯網系統安全創新之路」研討會
三、維運公部門連結小組		
辦理公部門連結小組會議	公部門連結小組會議分別於 3/13 及 6/30 召開，共計 2 場次。除 MWC、3GPP 會後分享外，並將國內 6G 產業技術使用頻寬之發展及基本資料調查結果，	公部門連結小組會議已於 9/14 及 12/12 召開。除 EuCNC 2023 會議、112 年國際組織參與推動概況及第 2 屆點子松成果分享外，針對 113 年公部門連結小



期中期末進度 工作項目	期中報告產出	期末報告產出
	建置於頻譜資訊協作平臺，作為各工作組產業發展之參考。另就各工作組 112 年下半年業管計畫辦理之座談或推廣活動，進行盤點和活動串聯可行性評估。	組會議之規劃方向進行報告，有助於各工作組未來計畫整合協調。
協助國際標準組織參與及建立國際合作管道/案例	已建立共計 3 案國際合作管道： 1. MWC 2023 行前交流會 2. MWC 2023「行動通訊大展重點趨勢研討會」及「預見通訊智能新未來研討會」 3. 6G 國際組織參與支持機制提案徵選	蒐整 113 年度國內外行動通訊相關國際會展會議。
觀測國際應用服務展及國內產業能量盤點	每月辦理公部門電子報發報，截至 7 月止，共計發報 6 期電子報，其中成果報告共計 4 則。	每月辦理公部門電子報發報，截至 11 月止，共計發報 11 期電子報，總計 115 則國內外活動及重點成果報告，以及時掌握 6G 技術及趨勢發展。

資料來源：本計畫整理

第二章 建立 6G 跨領域應用情境之參考架構先導評估

6G 通訊技術被認為是未來網路發展的關鍵，能支援更高的傳輸速率、更低的延遲、更廣的覆蓋範圍、更高的可靠性和更好的安全性，且將支援更多設備之間的溝通，使得資料更多元。

首先第一節將深入探討 6G 應用標準趨勢與進程，透過參考國際電信聯盟無線電通訊部門(International Telecommunication Union Radiocommunication Sector, ITU-R)的研究討論和建議，以及基於服務應用的演化趨勢，本計畫將研析下一階段全球行動通訊的願景，這將有助於整理和歸納出 6G 的應用情境與整體系統目標。在 6G 應用標準的趨勢與進程中，能發現對於更高性能和靈活性的需求。

其中，Cloud-Native 技術被廣泛應用於網路功能虛擬化(Network Function Virtualization, NFV)，將網路功能拆分成輕量級的虛擬化單元，這提供了更大的靈活性和高度虛擬化。同時，AI-Native 被視為未來 6G 行動系統的核心架構特徵之一，強調了 AI 的重要性。因此第二節蒐集研析 Cloud-Native 6G 及 AI-Native 6G 之跨領域應用情境參考架構，本計畫將探討如何在不同領域應用 6G 技術，以滿足不同的通訊性能和資源需求。這些參考架構可以幫助理解如何將 6G 技術應用於不同的領域，從而滿足不同的通訊性能和資源需求。此外，也將分析在這架構下有哪些 6G 跨領域應用及其帶來的挑戰，並研究如何運用協同分析(如 FL)解決問題。

6G 環境預計會有大量跨領域的新應用情境不斷湧現，這將使得通訊需求不斷增長，以及系統能夠靈活地適應多樣化應用場景的需求。因此，在第三節跨應用層和網路層的通訊強化機制研析與方法中，本計畫將深入研究如何強化通訊在不同應用場景下的效能。不同的應用場景對通訊性能和資源需求有不同的要求，因而需要制定 6G 技術的規格和標準，以實現跨應用層的通訊支援和網路層的優化。此外，為

使通訊系統能夠靈活地適應新應用場景的通訊需求，技術的發展將關注在更廣泛的應用場景和需求。這可能包括不斷增長的應用類別，需要在模型中動態引入新的類別來適應變化。在每個應用場景都可能對通訊系統提出新的要求情況下，傳統的學習系統可能需要不斷調整和擴展，以適應新的通訊需求。

第四節跨領域應用情境實證與雛型系統先導評估將探討如何實際應用 6G 技術於多樣化應用情境中，而聯合新增類別學習方法的使用，可以被解釋為在 6G 網路中支援新的通訊需求和應用的一種策略：允許系統在不中斷運行的情況下，動態地學習和適應新的應用類別，從而保持對不斷變化需求的支援，與 6G 技術在支援新的應用時需要具有的靈活性相呼應。因此，將跨領域應用情境實證部分視為一種探索，用來應對 6G 時代多樣化應用情境的方式。這類的方法可能在 6G 技術發展中成為一種重要的技術支援，以實現對於新型態應用的即時適應和高效通訊。藉由智慧商店商品辨識中新增類別的應用情境進行跨領域實證，並使用 CIL 進行模型訓練和更新。目標包括在跨設備和分散式環境下進行模型訓練和更新，確保新增類別不會影響既有類別的辨識率，且模型能夠持續辨識新類別。透過實驗設計比較 CNN 和 CIL 2 種模型的性能，包括運算時間比較、測試正確率和錯誤案例分析等，提供 2 種模型的性能優缺點，可以根據特定應用需求來選擇適當的模型。同時開發一款具有 3 個主要功能的應用程式(Application, App)，包括「模型應用」、「新資料上傳」和「產品內容」。在「模型應用」功能中，使用者可以上傳圖片，並顯示模型的預測結果。在「新資料上傳」功能中，使用者可以上傳新的類別圖片以進行模型訓練，提供一個清晰的流程，包括輸入相關資訊、上傳圖片、開始訓練等步驟。最後，「產品內容」功能讓使用者可以查看可辨識的商品類別。

第一節 6G 應用標準趨勢與進程

5G 行動通訊系統為 ITU-R 依據全球國家決議於 2020 年所完成之標準系統，該無線電標準系統為一個能支援各種應用，具有彈性及多種發展可能性之網路系統，將帶動全球資通訊產業與網路系統之布建與產業發展之進程^{2.1}。對於 2030 年下階段全球 6G 行動通訊系統之實現，全球產業皆普遍認知將延續 5G 發展架構與概念，持續改造目前資通訊產業環境與商業模式。在 ITU-R 之後續規劃下，隨著 6G 應用更極致化的應用需求，6G 技術亦將根據各種不同應用場景，實現各種專屬之技術方案，以迎合 6G 時代之新服務需求。

參酌 ITU-R 研究討論與建議，從服務應用之演化趨勢出發，研析下階段全球行動通訊願景，並據以整理歸納 6G 應用情境與系統總體目標^{2.2}。

一、6G 應用趨勢

在 ITU-R 所勾勒之全球未來資通訊願景下，6G 標準系統已經正名為 IMT-2030，並被賦予從行動通訊角度實現特定目標之任務^{2.3}。因此 6G 應用發展將朝向以下 9 大應用趨勢演進：

（一）智慧性普及（Ubiquitous Intelligence）

伴隨著 AI 與 ML 技術的進階發展與普及，AI 的使用將逐步成為未來各式應用的發展基礎，甚至更可預見 AI 成為簡化生活與促進社會發展的推進力，也就是 AI 將隨時隨地充斥在生活周遭而無所不在。未來的可連線裝置也將因具備各種感知資訊，成為民眾、機器與環境之間促進交互溝通的重要媒介與工具。此外，AI 除了可應用在網路系統，提供營運與管理最佳化之功能外，也可以用來

2.1 林咨銘，包偉丞，葉庭語，蔡峻嘉，周威宏，“全球 5G 標準系統與技術效能評估”，工研院電腦通訊期刊，第 181 期 5G 技術專輯，2020 年 3 月 17 日。

2.2 本章節資料來源，主要整理 ITU-R WP5D 第 44 次會議之相關討論與決議文件。（來源參考 <https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/Pages/default.aspx>）

2.3 ITU-R R19-WP5D-221010-TD-0740, “Naming for International Mobile Telecommunications”, WP5D #42, October 18th, 2022.

促進各種傳輸效能，以及針對使用者體驗之改善建議。整體而言，未來之行動通訊可將 AI 視為一種服務，並須具備一定之安全性與可靠性，以確保相關於使用者、系統與服務等元件的敏感性資料，不會在網路與裝置間傳遞時遭到竊聽、竄改或濫用。

(二) 普適運算 (Ubiquitous Computing)

經由 5G 行動通訊系統的發展，橫跨終端、基地臺、系統與網路之通訊運算將日漸成形，如此之趨勢將繼續延續至 2030 年。以此觀之，未來 6G 行動通訊將須將如此大量之通訊運算分散至各個網路或裝置，如此才有可能直接對每一用戶端實現低延遲且可靠之通訊傳輸與計算服務，尤其是需要大量運算且必須立即性反應之通訊應用服務。針對此類之應用發展，透過協調與平衡邊緣運算的網路與運算資源，形成通訊與計算適度融合之服務覆蓋，可將有效運用整體網路資源，以增加網路系統效能，提升使用者體驗。6G 特別需要此類網路服務之應用，如擴增實境(Augmented Reality, AR)與虛擬實境(Virtual Reality, VR)之成像(Rendering)，自駕車與運輸控管與導航，智慧鐵路與全息通訊等，皆須透過通訊與運算雲端邊緣之協調方能實現。

(三) 沉浸式多感媒體整合 (Immersive Multimedia and Multi-sensory Interactions)

未來的多媒體應用服務，將以在數位世界中，提供使用者沉浸式(Immersive)的感官與虛擬互動體驗為主，因此混合式實境(Mixed Reality, MR)與全息遙控(Holographic Telepresence)將逐漸成為接下來的應用趨勢，倘若再加上沉浸式 3D 體驗，以及虛擬與實境的深度整合，將使沉浸多媒體成為未來工作與一般社交的重要日常規範。未來以使用者為中心的人機介面(Human-Machine Interface)更可整合 XR，透過快速的遠端通訊與即時的虛實反映平臺，提供更多感(Multi-Sensory)的沉浸式體驗，完整實現各種遠端

艱難的操控與分身作業，經典應用包含遠端手術(Telesurgery)與遠距操控傳輸(Remote Transportation Control)等。此外，沉浸式多媒體也將徹底實現遠距工作，除了讓員工可完全居家上班(Working From Home, WFH)之外，老師與學生之即時授課互動也將不再受到距離限制，而極致完美的演唱會或其他娛樂活動也可在實體與數位整合之元宇宙(Metaverse)中被完整實現。

(四)數位孿生^{2.4} 虛擬世界 (Digital Twin and Virtual World)

未來 6G 的世界已經被期盼透過即時通訊與數位孿生來促進實體與數位世界之整合，而數位孿生之實現，也必須藉由隨處可存取之感知、智慧以及通訊裝置平臺，來提供包含監測(Monitor)、設計(Design)、管理(Management)、分析(Analysis)、診斷(Diagnosing)、模擬(Simulation)、導航(Navigation)、互動(Interaction)等特性與功能。綜整來說，數位孿生所需要的實現技術，包含通訊與 AI、感知與計算的整合。此外，數位世界內之分身，則須倚靠信賴通訊來與實體世界之感測元件做最即時無縫的反應回饋。未來應用數位孿生的 6G 應用，包含數位農業(Agriculture)、數位工業(Industry)、數位建設(Construction)、數位資產(Estate)管理，數位智慧城市(Smart City)等。未來在順應數位孿生的發展風潮下，許多協助虛實整合之網路系統也已正在開發研究當中，目標在結合網際網路、實體與使用者空間，以提供真正完美之使用者體驗情境。

(五)智慧工業應用 (Smart Industrial Applications)

在 5G 行動通訊系統發展的過程中，機器與機器的協同合作通訊已經逐漸成為未來智慧工廠的趨勢發展基礎，再加上 AI 與數位孿生的技術整合，智慧裝置與機器人已經具有可取代人類進行各式工廠作業的潛力。伴隨著生產製造作業經驗的累積，配合著資訊即

2.4 依據 ITU-T 建議書 Y.4600 之定義，數位雙生專指一個可在某一數位應用或情境中，代表特定之實體主客體，且可即時同步連動之數位物件。

時的傳遞與機器間協同合作，可快速有效率實現智慧生產的工廠已經逐步成形。未來若再配合上中下游產業的技術整合，以及即時的指示命令，可完全替代作業人員的數位人類(Digital Human)，其面世亦指日可待。此種類之技術整合與服務應用，不只是可以應用於封閉之工廠內，亦可在開放或移動之作業環境中實現，例如自駕車、其他需要許多彈性、即時反應或協調互動之使用場景。

(六)數位醫療^{2.5} 照料 (Digital Health and Well-being)

在 5G 行動通訊系統的發展下，現行網路已經可以透過精準、可靠、低延遲與高傳輸效能，提供基本之電子醫療服務。隨著近年來多存取邊緣運算(Multi-access Edge Computing, MEC)技術的快速發展，更可進一步提升公眾電子醫療服務的服務品質與安全性。若能進一步完成實體與虛擬實境技術的整合，將可透過提供沉浸式體驗，完成更精準且艱難的醫療任務。因此，對安全與可靠要求更為嚴謹之身體網路，與各式提供細微精準的生化感測元件，將成為此應用的重點項目。此外，全球已經歷過 COVID-19 嚴重特殊傳染性肺炎之洗禮，對於遠距電子健康醫療服務的迫切需求又更勝以往，未來此類的可能新興服務，包含遠距診斷(Tele-Diagnosis)、遠端照護(Remote Healthcare)、電子人工感測器(Electronic Artificial Sensor)、數位臨床試驗(Digital Clinical Trials)與遠距復原(Tele-Rehabilitation)等。在此同時，聯合國組織也呼籲未來民眾的心理健康(Mental Health)與營養等議題，也有必要透過 6G 系統來提供全面覆蓋且可負擔之行動通訊來應對。

2.5 依據 WHO 研究報告“Global strategy on digital health 2020-2025”，數位醫療包含各種透過電子與網路技術，可用來改善醫療照顧服務與環境之數位科技，包含物聯網，人工智慧，與機器人等。

(七) 普適連結 (Ubiquitous Connectivity)

廣域無縫隙的無線電訊號涵蓋，除滿足基本的使用者通訊需求之外，亦可提供如教育、健康、交通、重要商務與緊急的必要服務等。進一步說明，透過有效率且可負擔之方式，將全球所有尚未連結(Unconnected)區域的設備或裝置提供服務涵蓋，將可透過廣域無縫隙涵蓋具體實現數位包容(Digital Inclusion)。由於數位包容必須為各式位於遠端、疏遠或艱困地區之社群，提供有意義之連線支持，為無所不在智慧行動社會的關鍵目標，因此也將會是未來 6G 重要願景之一。為實現此願景目標，整合現存或具發展潛力之地面(Terrestrial)與非地面網路(Non-Terrestrial Network, NTN)系統，如衛星與高空平臺，並完成與連線整合與互通，將會是接下來提供廣域無縫隙涵蓋的發展重點。

(八) 感測通訊整合 (Integration of Sensing and Communication)

感應偵測與通訊整合是現今無線通訊的重要發展趨勢，若再配上高解析與精準之成像、定位與對應之系統能力，將可進一步促進物體偵測、移動感知、以及其他需要對距離、角度與移動速度有需求之超高精準服務之實現，甚且所感測之資料又可透過在不同裝置或第三方設備之通訊與共享，在特定區域提供客製化之應用服務。此外，若整合區域所提供之定位、感知與影像資訊，再配合 AI 的處理分析，將更可進一步實現全意境感知(Full Context Awareness)之進階服務。透過交換智慧感測資訊所形成之連線智慧(Connected Intelligence)，對於促進實現虛實整合之應用服務也有相當大的幫助。未來此類的應用服務，包含即時 3D 顯像、遠距自駕車或運輸、機器偕同合作、環境與產品製造監測等。

(九) 永續發展性 (Sustainability)

行動通訊一直以來維持著全球經濟之發展，而為了全人類的永續發展，聯合國亦已設下目標，包含環境保護、弭平數位落差、碳

排中和、減緩氣候變遷等。因此，未來有助於維持永續發展目標的新興應用，都將成為下階段全球發展的重要應用趨勢，也成為 6G 行動通訊系統的發展契機。緣此，6G 行動通訊系統需朝向節能減碳之方向戮力進行，包含提升能源使用效率、採用環境友善之材料、高效布建網路與運作、朝向效能(Efficiency)、花費(Cost)以及永續性之平衡發展。此外，透過穩固的電信架構來協助各種可能自然災害之防範與救難，也是促進永續發展目標的其中一環。

二、6G 應用發展情境

自全球行動通訊系統發展以來，一直以通訊與影音等個人行動寬頻為主軸，如 3G 開啟行動通訊(Mobile Communication)服務，4G 提升行動寬頻(Mobile Broadband)，而 5G 更是進一步提升使用者體驗及至各式應用，開展增強行動寬頻(Enhanced Mobile Broadband, eMBB)、大規模機器型通訊(Massive Machine Type Communications, mMTC)與超可靠低延遲通訊(Ultra-reliable and Low Latency Communications, uRLLC)等 3 大應用場景。依據前述章節所整理之 6G 應用發展趨勢，6G 應用除繼續延續發展原本以人為中心(Human-Centric)之使用情境外，又因可再進一步結合人與人(Human-to-Human, H2H)、人與物(Human-to-Machine, H2M)與物與物(Machine-to-Machine, M2M)之需求，ITU-R 於第 44 屆 ITU-R Working Party 5D (WP 5D)會議上定稿之 IMT-2030 (6G) 新建議書中，再擴增至 6 個主要應用情境如圖 2：

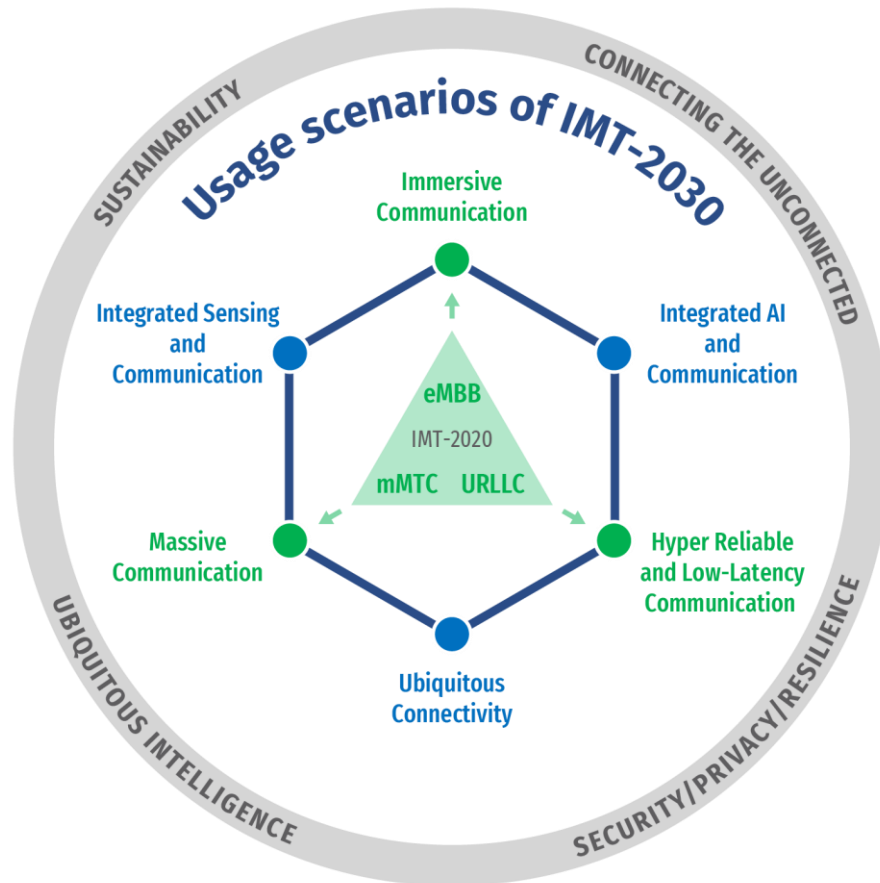


圖 2、6G 使用情境與系統發展架構

資料來源：請參閱附錄-參考資料^{2.6}

(一) 沉浸通訊 (Immersive Communication)

此應用情境源自於 5G 行動通訊之行動寬頻使用情境，涵蓋未來人與機器間的各種互動通訊之需求。典型之應用包含 XR、全息通訊(Holographic Communications)、遠端多感遙控(Remote Multi-sensory Telepresence)、工業機器人控制與回饋等，而可獨立運作之語音服務也有可能整合進入沉浸行動寬頻中。

透過如智慧眼罩等新型通訊裝置開發設計，將逐步改變傳統行動寬頻之通訊方式，改以資訊的取得與互動傳輸為主。此外，針對周遭環境快速且高密度的取樣，網路端將必須擔負起相關資料的高

2.6 ITU-R R19-WP5D-230612-TD-0905, “Framework and overall objectives of the future development of IMT for 2030 and beyond,” WP5D #44, June 22th, 2023.

速通訊與繁雜計算，如此才有可能在遙遠的端點，透過即時數位成像來完美實現沉浸式應用。

此應用情境將需要網路系統提供高速及低延遲之傳輸速度，以及較高之網路通訊容量，而可能的使用場景包含各式密集都會與郊外地區。

(二)超極可靠低延遲通訊 (Hyper Reliable and Low-Latency Communication, HRLLC)

此應用情境延伸自 5G 行動通訊之高可靠低遲延通訊使用情境，包含各式對於傳輸可靠度與延遲有著極高需求之應用，並對可用性 (Availability) 有著更進一步的要求。此類情境也適用於其他可信賴計算 (Dependable Compute)、物件之精準定位 (Accurate Positioning) 與表徵 (Characterization)、AI-Native 資料傳遞散布等。

典型的應用包含可擴展距離與實現自動化生產之智慧工廠，可遠距操控和自動駕駛之智慧車輛與車隊，可透過偕同相互合作並完成一般人無法完成任務之智慧機器人，可即時接受使用者指令完成 H2M 人物互動任務之無人機群，以及其他需低延遲、可用且可信賴通訊的遠距照護、診斷以及手術之智慧醫療。此類應用考量的重點，在於避免因為通訊延遲或失敗，而可能衍生安全問題，或甚至引發生命危害的可能性。

由於此情境之應用非常倚賴特定應用專屬之環境與場景，因此有可能發生影響的需求，包含有資料傳輸率、傳送延遲、延遲變異 (Jitter)、電耗條件與裝置連線密度等，而其中每一個需求皆有可能在特定情況下成為關鍵性之影響要素。

(三)巨量通訊 (Massive Communication)

此應用情境繼續強化自 5G 行動通訊之 IoT 使用情境，目標在迎合未來逐漸普及的 IoT 網路，尤其是對於那些位處大範圍環境，

對耗電與使用時間都有著高需求、低價及大量之 IoT 裝置。若在持續演進發展之下，對於移動性與寬頻傳輸亦可能有更進一步需求。

此類可能之應用，包含工業生產所需龐雜的感測與物料監控，智慧城市中關於安全、交通與環境等各種大量監測追蹤。此情境所需面對問題，除了更大量裝置數量外，又更進一步強調分布與地域性，尤其是所可能涵蓋之範圍，諸如水壩、橋梁及隧道山洞等環境。此外，物聯裝置功能的差異性，例如傳輸率、耗電、移動性與穩固性等，都是必須考量的重點，甚至在某些特定遠距區域，也必須將裝置的維護成本考慮進去。

此類型應用情境雖然包含多樣應用，但卻有著共同特徵需求，即是對於物聯裝置的全向可現性(Omnipresent)。5G 以 IoT 的連線裝置數量，作為系統發展與佈建之需求。然而，即使數量達一定規模或量級，並不代表通訊服務的無所不在。因此，6G 強調除裝置數量外之進階需求，也就是希望達到無所不在之 IoT 網路。至於更具體或是量化之需求，仍待進一步的討論與確認。

(四) 普適連結 (Ubiquitous Connectivity)

為全世界普羅大眾提供可負擔的行動通訊是 2030 年很重要的發展目標，因為無遠弗屆的全域行動通訊將有助於發展數位平權 (Digital Equality)，使得一般民眾皆可在財務性 (Financial)、實體性 (Physical) 與地域性 (Geographic) 接收可行條件下之網路服務。下世代之行動通訊，必須從各個面向來持續改進，包含系統架構、通訊裝置、無線存取、網路回傳、訊號覆蓋與功耗效率，並從生態面、經濟面以及社會面來進一步促進全人類永續發展目標。

此使用情境必須同時從水平與垂直角度來考慮各式有助於實現永續發展目標之應用，尤其是溫室氣體 (Green House Gas, GHG) 的排放偵測，與氣候變遷 (Climate Change) 所導致的災害偵測與預防。為此，可負擔以及隨處可得之連線服務，有助於實現遠距資訊

傳遞與教育推廣，而將成為下階段行動通訊發展的另一個重要需求。在現今全球新冠疫情消退，經濟活動正緩步回復之情況下，全域行動連線對全世界未來發展的重要性不言可喻。

此類型應用情境所追求的是在任何地域皆能存取基本通訊能力，包含上行與下行的訊號涵蓋與一定之傳輸速率，而行動裝置的連線時間與能源效益也是一個重要因素。此外，在前述條件下無縫(Seamless)連線維持與使用者體驗，皆是必須考量的重點。

(五)AI 整合通訊 (Integrated AI and Communication)

此應用情境包含 2 種發展需求，一是符合 AI 需求之網路(Network for AI)，另一則是 AI 加持之網路(AI Powered Network)。前者指可促進 AI 運行之網路環境，藉由傳遞交換資料模型或學習資料，來促進 AI 實現各種複雜之應用服務，後者則是透過 AI 的輔助運算，來進一步改善提升網路傳輸效能與安全性。

無論 AI 需求網路或是 AI 加持之網路，皆必須透過分散於網路各處之智慧節點(Intelligent Agent)，來偕同進行大量學習資料交換，以取得最佳解答完成服務。此類潛在應用，包含影像收集辨識、創造與識別數位孿生，偕同完成困難任務之機器人，工廠設備流程自動化，H2M 人機介面的精準學習與改善。

若以通訊面向來討論 AI 網路，一定區域內之網路系統容量與適當之使用者體驗資料傳輸率，仍是基礎需求，而針對各式 AI 所驅動的應用服務，網路系統亦須具備相當之低傳輸延遲與高可靠性。此外，有別於其他應用情境，AI 網路需要考慮一些不同以往之系統能力與需求，並重新定義，例如安全性、資料隱私(Data Privacy)與可解釋性(Explainability)，皆是此應用情境所必須考量之需求。

(六)感測通訊整合 (Integrated Sensing and Communication)

感測通訊整合指的是結合眾多感測所取得之資訊，透過無線通訊網路偕同整合交換通訊，來提供更多面向之感測結果，藉此實現

各式對於定位精準或解析度要求更高之應用服務。未來網路系統，透過延用既有或新開發感測元件與裝置，配合低延遲之整合通訊，即可在實體物件與虛擬物件間，實現即時對應成像與互動溝通。

此類應用服務，基本包含 H2M 人機介面所需之姿勢與手勢辨識、物件辨識追蹤、數位成像(Imaging)與對應(Mapping)。若完整結合各式感測元件，可同時轉化如意象、手勢、墜落、移動、顯現等多重感知通訊，將可成為未來商務與工業重要應用，並可廣泛應用於智慧家庭、智慧工廠、智慧城市與互動式體驗或觀覽。

感測通訊整合無疑為結合實體世界與數位世界之重要應用情境，其所需之需求包含感測靈敏度、解析度、速度與角度，以及定位之精準度與信心度，而此需求也將隨著不同應用服務的特性呈現不同重要性。

三、電信商對 6G 標準發展進程

根據工研院產業情報網蒐集資料指出，2022 年全球通訊產業市場可達 2.19 兆美元，疫情催化企業數位轉型，企業內資料中心也逐漸由本地轉往雲端，或推出 Cloud-Native 新應用服務，使得 2022 年總體市場成長 3.7%，故在通訊設備產品方面包含 5G 電信核網端、雲端高速交換設備、商用廣域/區域網路、無線區域網路、數位用戶線路（Digital Subscriber Line, DSL）及光纖寬頻網路等應用產品，在低軌衛星通訊題材以及 5G 專網、雲端應用等議題發酵下，預估 2023 年全球通訊產業年成長率為 4.5%，達約 2.29 兆美元。而在此國際通訊產業基礎上，預估 2023 年臺灣通訊產業年成長率為 1.6%，達約 435 億美元。

國際通訊標準組織 3GPP 今(2023)年 6 月 13 日至 16 日於臺北舉辦 3GPP Release-19(R19)標準研討會，收集分析全球電信大廠對未來 6G 標準的看法，其中電信大廠諾基亞(Nokia)如圖 3、易利信(Ericsson)如圖 4、電信晶片大廠高通(Qualcomm)如圖 5、手機大廠樂金(LG)

如圖 6 與索尼(SONY)如圖 7 對 6G 標準發展的進程略有差距。但國際電信領頭廠商一致認為 3GPP R19 標準為連接 5G 標準到 6G 標準的橋樑，緊接著在 3GPP Release-20 (R20)標準開始研究 6G 標準的服務與系統(Services and Systems Aspects, SA)與無線接取網路(Radio Access Network, RAN)需求，並於 3GPP Release-21(R21)標準開始制定第 1 階段的 6G 標準。

Nokia 預估從 2020-2030 年 6G 處於萌芽階段，如圖 3，在下一個世代初站穩腳步，然而頻譜是無線寬頻行動通訊的命脈，如果無法及時獲得正確的頻譜，6G 大部分應用場景將無法實現，Nokia 主導的 Hexa-X 和 Hexa-X-II 3 等世界各地的研究計畫正在開發下一代網路的關鍵技術，ITU-R 第 4 屆會議將透過世界無線電通訊大會(World Radiocommunication Conference, WRC)決定 6G 的頻段和條件。除了 ITU-R 之外，3GPP 還需要就標準化要求達成一致，第一個 6G 規範預計將於 2028 年 3GPP R21 中發布。2023 世界無線電通訊大會(WRC-23)(預定於 2023 年 11 月召開)可能就 6G 研究的候選頻段做出決定，這將影響 2030 年之前研究發展藍圖。

現我國已投入學研資源，關注 6G 發展中的安全問題，預計於 2025 年完成雛型系統(Trial System)，並於 2028 年啟動 6G 商用實驗專網，建立我國通訊產業及技術之國際優勢，發揮國際影響力。

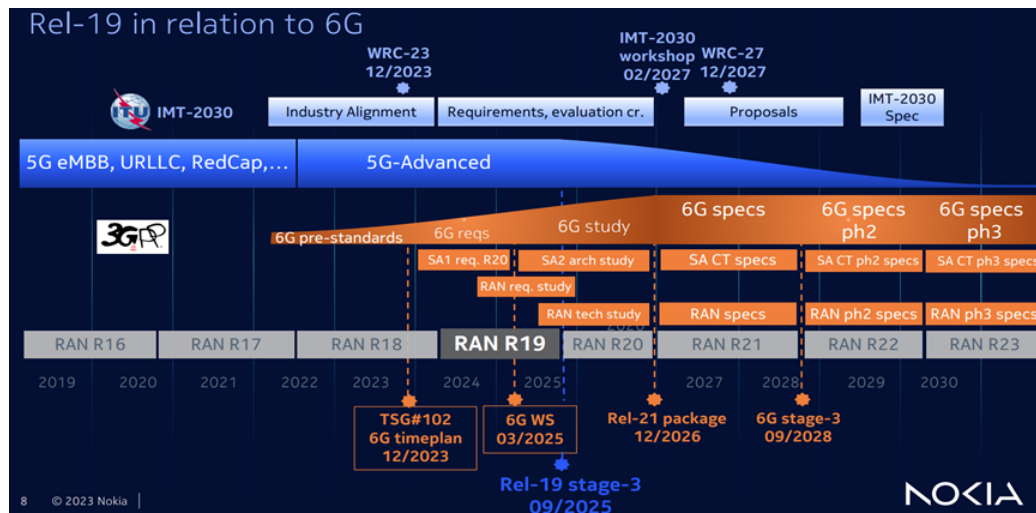


圖 3、Nokia 發布 6G 標準演進時程

資料來源：請參閱附錄-參考資料^{2.7}

Ericsson 於 2021 年起主導北美洲地區 Next G Alliance，推測 6G 基礎技術的早期標準會在 2024 年發布，第一個可實施的 3GPP 6G 規範將於 2028 年推出，並在 2030 年進入商用化階段，如圖 4。

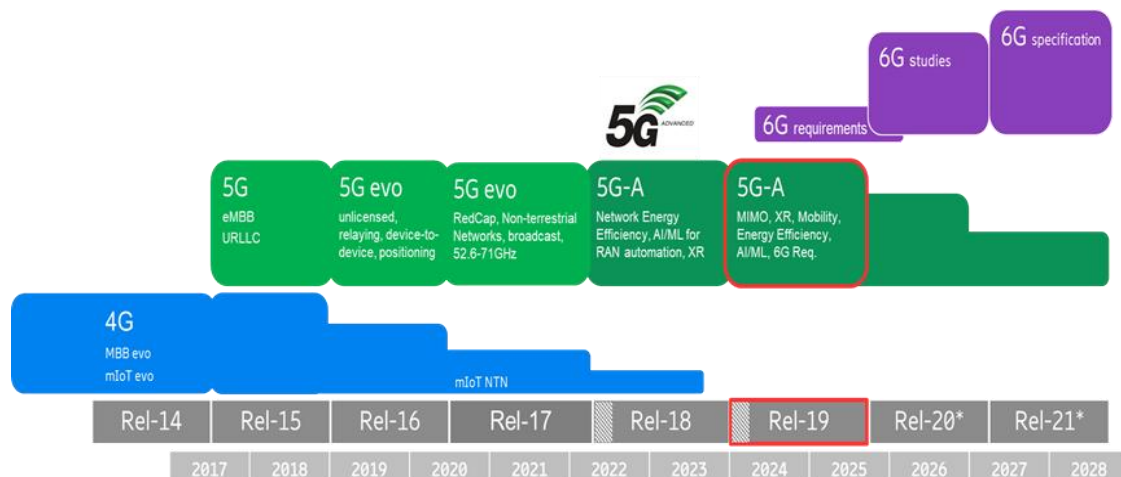


圖 4、Ericsson 發布 6G 標準規劃時程

資料來源：請參閱附錄-參考資料^{2.8}

Qualcomm 考量 2024 年起，通訊標準將從 5G Advanced 到 6G 的過渡，技術上探討如何使用服務代理程式等 Cloud-Native 解決方案，

2.7 3GPP RAN Release-19 workshop, RWS-230012

2.8 3GPP RAN Release-19 workshop, RWS-230147

來限制對遺留部署的影響而不影響互通性，如圖 5。預估在 3GPP R20 將開始進到原生 AI 技術，晶片在設計上融入 AI 運算，預期在 2027 年整備的 6G 標準，將可透過共址在邊緣託管網路功能，以及多傳輸層和無線接取技術頻譜動態共享 (Multi-RAT Spectrum Sharing, MRSS)，實現共享雲端、運算、和儲存資源的商機。

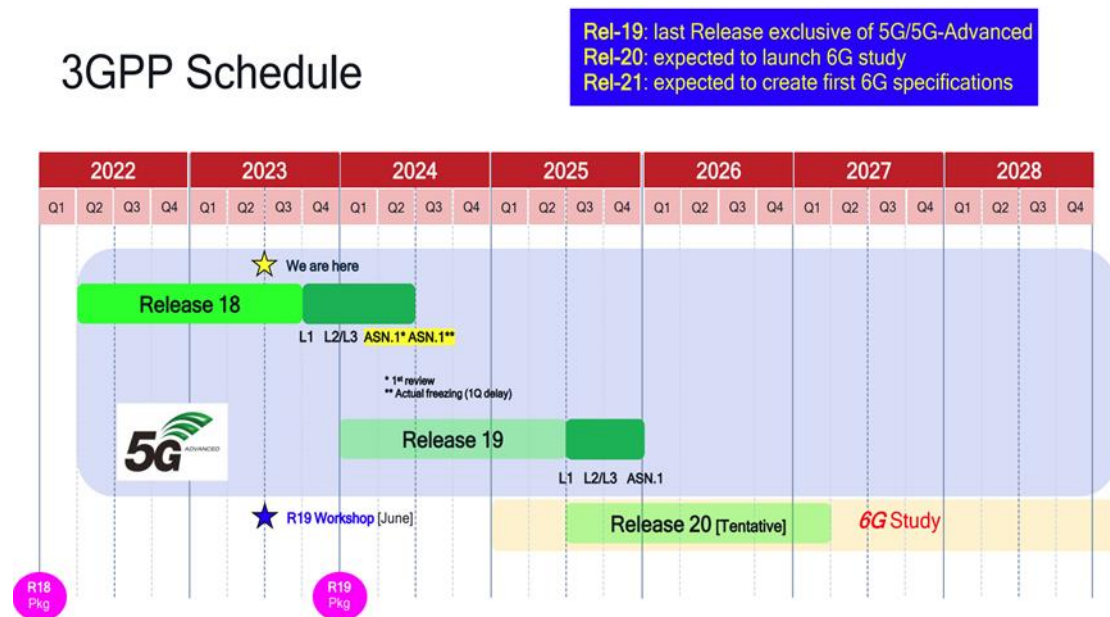


圖 5、Qualcomm 發布 6G 標準規劃時程

資料來源：請參閱附錄-參考資料^{2.9}

2019 年 LG 與韓國科學技術院 (Korea Advanced Institute of Science and Technology, KAIST) 共同建立 LG 電子-KAIST 6G 研究中心，LG 陸續與德國弗勞恩霍夫研究所、KRISS 和是德科技等多家機構建立了研發合作夥伴關係，共同開發 6G 核心技術。

韓國政府規劃在 2024 年啟動開發未來 6G 系統計畫，LG 在其中發展比 5G 更快的數據速度、更低的延遲和更高的可靠性，將能夠帶來環境萬物聯網 (Ambient Internet of Everything, AIOE) 的概念，為使用者提供增強的連結體驗，並配合韓國政府啟動尚未標準化的 6G 行

2.9 3GPP RAN Release-19 workshop, RWS-230264

動服務試點計畫，LG 的目標是 2026 年展示 Pre-6G 技術，6G 預計將於 2029 年實現商用，如圖 6 所示。

• Rel-19 time schedule should be kept tightly

- The Rel-19 completion time is closely related to the start of Rel-20, when the 6G study is expected to begin
- Workload of Rel-19 should be controlled moderately to be completed on time within 18 months per WG

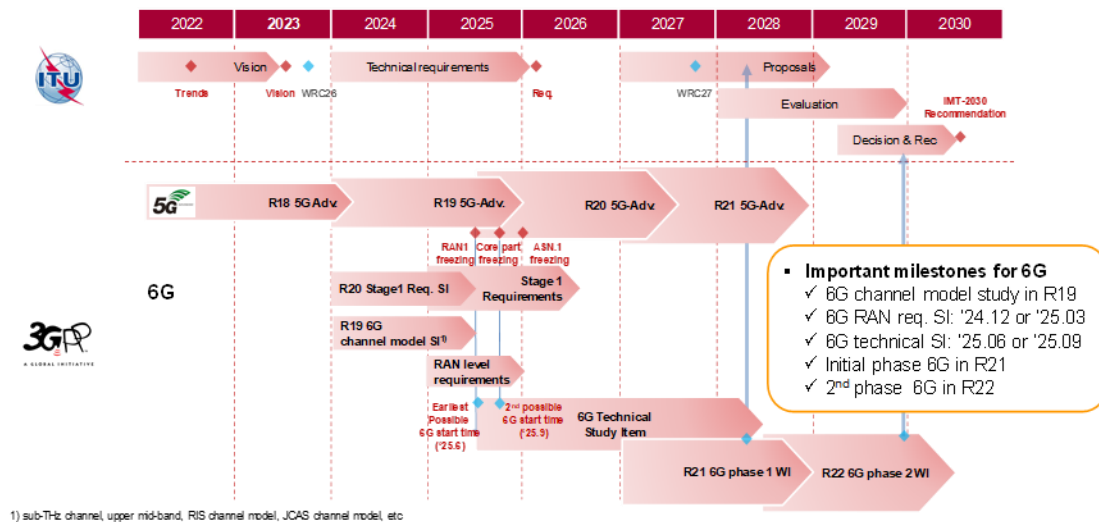


圖 6、LG 發布 6G 標準規劃時程

資料來源：請參閱附錄-參考資料^{2.10}

日本政府於 2020 年 12 月成立 Beyond 5G 推動聯盟，促進產學研政府在 6G 技術方面的強而有力及積極的合作，SONY 是其中廠商成員，並致力於 3GPP 等國際標準化的理論研究、模擬器開發和技術提案，探索動態頻譜共享等創新技術，以更好地利用頻率資源，透過試驗臺開發和示範實驗實現商業化，預計將在 2030 年實現 6G 推動示範實驗和國際標準化，如圖 7 所示。

在 2030 年前，6G 技術開發將成為眾多產業經濟發展的重要驅動力，相較於先前通訊世代，在 6G 技術發展中整合雲端、AI 等不同領域技術已成為共識，由於 6G 願景必須涵蓋多元複雜之應用情境，須以跨界協作方式，整合不同領域技術將有助於強化 6G 技術之廣泛適用性。

2.10 3GPP RAN Release-19 workshop, RWS-230192

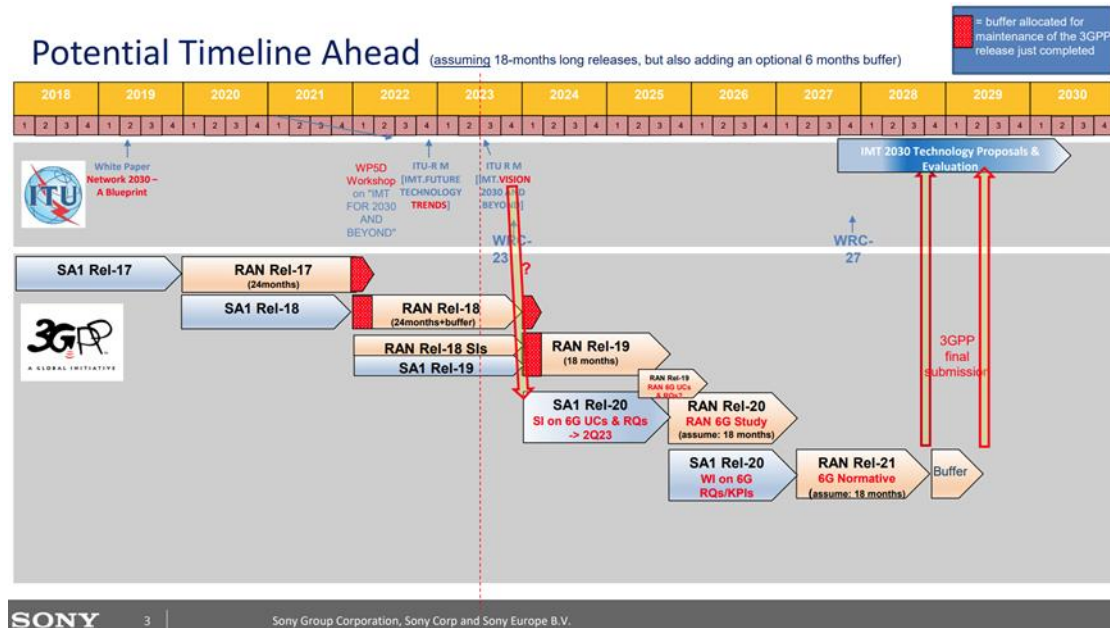


圖 7、SONY 發布 6G 標準規劃時程

資料來源：請參閱附錄-參考資料^{2.11}

2.11 3GPP RAN Release-19 workshop, RWS-23090

第二節 蒐集研析 Cloud-Native 6G 及 AI-Native 6G 之跨領域應用情境參考架構

本計畫藉由蒐集研析 AI-Native 6G 和 Cloud-Native 6G 之跨領域應用情境參考架構，探討 2 種架構在不同應用場景下的運作和特徵，以及對於 6G 技術跨領域應用的影響和優勢。

未來 6G 將會需要更靈活且高度虛擬化的網路基礎設施，以支持不同的應用和服務。Cloud-Native 概念可以應用於 NFV，將網路功能拆分成輕量級的虛擬化單元，並使用容器技術來部署和管理虛擬化功能，即網路作業無須安裝新的硬體，就能動態提供新的服務。而安全的考量容器技術原生特點之一，相對的針對運作於容器的應用服務也提供相當的安全防護，可強化 6G 是各種應用的安全與隱私防護。

AI-Native 被業界認為是未來 6G 行動系統的核心架構特徵之一。基於電信基礎設施普及之現實優勢，網路運作效能以及能源使用效能是 6G 運作必考量的重點，而其 AI-Native 的特徵，在蒐集行動網路上的資料，架構於 AI 的功能動態配置頻寬、功率、儲存等資源，以提供網路的效能、節能的效益，更加彰顯出 AI 效能提升和價值，協助實現未來 6G 無線網路的願景實現。

一、Cloud-Native 架構、運作、特徵說明：

雲端原生運算基金會(Cloud Native Computing Foundation, CNCF)對 Cloud-Native 做的定義，「雲端原生技術幫助公司和機構在公有雲、私有雲和混合雲等新型動態環境中，建構和執行可彈性擴充套件的應用。雲端原生的代表技術包括不可變基礎設施(Immutable Infrastructure)、服務網格(Service Meshes)、宣告型 API(Declarative API)、微服務(Microservice)和容器(Container)。這些技術支援彈性、可管理和可觀察的鬆散耦合(Loosely Coupled)系統與自動化相結合，允許工程師們以最小的工作量頻繁地、可預測地做出變更。」，即一種在雲端運算環境中建置、部署和管理應用程式的軟體方法。企業可

藉以建置有彈性、可擴充和靈活的應用服務，提供快速更新應用服務內容，滿足客戶需求。

其中所謂不可變的基礎設施、服務網格、宣告型應用程式介面 (Application Programming Interface, API)、微服務及容器皆為 Cloud-Native 重要技術特徵。此外，Cloud-Native 在虛擬化做法除容器外亦包含虛擬機器，亦納入本節研析內。這些重要技術特徵的功能描述如下：

(一)不可變的基礎設施

不可變的基礎設施是指在部署和管理應用程式時，將基礎設施的狀態設定為不可更改或不可變的。意味著一旦基礎設施建立並運行，就不再對其進行直接修改，而是通過創建全新的基礎設施來進行更新或部署。即應用程式、配置和相關資源都被打包成可重複部署的映像檔(Image)，每次更新應用程式或配置更改時，都會建構新的基礎設施實例，此實例是從映像檔中創建，確保每次部署都在乾淨的環境中進行，而舊基礎設施則會被棄用或銷毀。直觀來說，程式被部署時，不希望再去做任何改動，當必須部署新的生產程式時，將對某個二進位映像檔進行抽換，而不是對於程式改動。同理，如果要還原到前版本，也是基於映像檔的抽換。

(二)服務網格

服務網格一種用於管理和維護微服務架構中通訊的解決方案。在微服務架構中，應用程式被拆分為多個小型服務，每個微服務可以獨立運行並相互通訊。服務網格提供一種集中管理服務間通訊的方式，以增強安全性、可觀察性和可靠性。以 Kubernetes(簡稱 K8s)為例，隨著專案越來越複雜，Kubernetes 中可創建和管理的最小部署運算單元 Pod，其數量會越來越多。而 Kubernetes 不會了解 Pod 的溝通行為，若其中一個元件出狀況，管理者往往都須花費很多時間才能找到問題，而服務網格負責處理服務溝通通訊，Pod 之間的

請求皆需通過此層，透過集中化管理，能蒐集 Pod 的連結情形，或是設置 Pod 之間路由規則，使其在不修改服務的情況也能達到流量管理、可觀測性等功能。

(三)宣告型 API

宣告型 API 讓軟體開發者可以通過定義期望的結果，或最終狀態來描述 API 的使用，而不需要指定具體步驟去實現目的。宣告型 API 讓開發者專注於描述「要做什麼」，而不用明確指示「如何做」，廣泛應用在許多場景中，特別是在設定和配置管理、雲端基礎設施部署、網路路由設定及資料庫查詢等領域，也與一些自動化工具和平臺密切相關，例如 Kubernetes 的 Pod 描述等。

(四)微服務

開發者要使用本質上支援雲端基礎設施的現代工具和技術進行應用程式開發。Cloud-Native 技術對於應用程式進行快速且頻繁更新，而不會影響應用服務的提供。

與傳統應用開發方式的差異在於，以往程式開發人員需要開發大量軟體功能，所有功能都完成之後再發布以進行測試。在效率上較不靈活，需要較長的時間來部署，而且無法快速擴展。

傳統應用開發方式與 Cloud-Native 的作法上有以下不同的差異：

1.架構設計

Cloud-Native 開發基本上會使用微服務架構，基於微服務的精神，將整體應用服務拆解為單一責任與功能的小型功能區塊為基礎，利用模組化方式組合出複雜的大型應用程式，每個區塊只專注於執行特定功能，各區間使用 API 進行通訊。若需要針對擴充或調整某一個業務功能時，只需要專注該業務功能的服務進行擴展即可，不需要對整個應用服務進行擴展、變更。

而傳統開發方式通常使用一個應用程式內包含所有業務所需功能的單機式架構，雖也能以分散式應用程式來實作，但在單機式架構，每一個業務功能都是不可分割的。若是要調整需要對整個應用服務作一個整體進行擴展，無法針對特定功能進行獨立擴展。

2.部署方式

Cloud-Native 開發基本上都會採用輕量級虛擬化的容器化技術(如 Docker)，打包和部署應用服務的程式運作環境等相關資料。容器提供一個獨立、可移植的運行環境，使應用程式能夠在不同硬體環境中順利運行，而傳統開發方式通常會使用虛擬機器(Virtual Machine, VM)或裸機部署應用程式，其中若是以裸機方式進行，可以獲得較佳的效率，但不容易移植到其他機器上運作。

3.自動化和可擴展性

Cloud-Native 開發強調自動化和可擴展性，使用如 Kubernetes 的自動化工具和程式來執行重複、繁瑣或容易出錯的任務。如容器部署和管理、彈性調整資源、故障恢復、監控告警等工作，減少手動干預和提高效率，從而提供系統更高的可靠性和可用性。同時系統能夠因應需求增長，投入更多資源來支援更大的工作負載。在 Cloud-Native 應用程式中，基本是以水平擴展，通過增加、容器或節點來分散負載，以滿足不斷增長的需求。傳統開發方式通常需要手動配置和管理部署環境，較難實現自動化和可擴展性。

4.彈性和可靠性

Cloud-Native 開發可讓系統根據工作負載的變化，彈性化自動擴展或縮減資源，以因應不同負載需求，以及面對故障和異常情況時保持正常運行，盡可能減少業務中斷時間，

提供穩定的服務可靠性。而傳統開發方式往往需要手動調整和管理資源，對於即時工作負載的變化，因應需求執行即時調整。

總體而言，Cloud-Native 開發方式強調可擴展性、彈性、自動化和可靠性，並使用容器和微服務架構來實現目標，讓組織能夠更好地利用雲端計算優勢，並更有效地建構和營運其應用服務。

另一方面，Cloud-Native 應用程式使用協作方法，可以在不同平臺上進行高度擴展。開發人員使用各種軟體工具，在 Cloud-Native 應用程式中大量自動化建置、測試和部署程式，團隊可以立即設定、部署或複製微服務，是傳統應用程式無法做到的。

透過虛擬化技術可以在硬體上創建一虛擬層來模擬實體運作環境，使得多個作業系統和應用程式可在同臺實體電腦上同時運行。將中央處理器(Central Processing Unit, CPU)、記憶體(Random Access Memory, RAM)、硬碟和網路等硬體資源進行抽象化和共享，提供更高的資源利用率和靈活性，實現應用程式的部署和運行，有效解決應用程式安裝到不同電腦的作業系統，與硬體資源配置所產生的不相容問題，所以虛擬化是實現 Cloud-Native 精神的重要基礎。

(五) 容器與虛擬機器

與圖 8 傳統應用服務使用的單機式架構不同，容器是以應用程式為單位的虛擬化技術，此稱為容器化(Containerize)，其特徵是將應用程式，所需如程式(Bin)及程式庫(Lib)等相關元件封裝於容器之中，執行容器管理、資源配置、網路、儲存管理、安全性和隔離性等功能如圖 9。目前廣為業界引用代表技術為 Docker 容器技術。

另一種 Cloud-Native 常見的虛擬化作法為虛擬機器技術，是一種以處理作業系統為單位的虛擬化技術，其架構如圖 10 所示，應用程式、所需各種相關元件及所使用的作業系統(Guest OS)皆包裝

於虛擬機器中，透過虛擬化管理程式(Hypervisor)根據基礎實體運算資源配置給個別的虛擬機器，VMware 為最典型的代表。

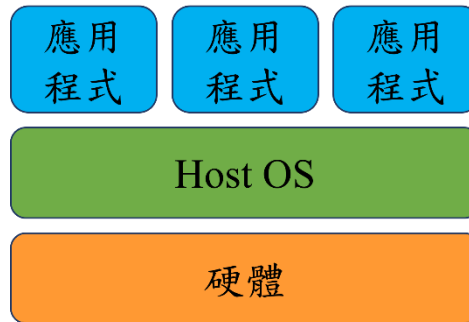


圖 8、單機式架構圖

資料來源：本計畫整理

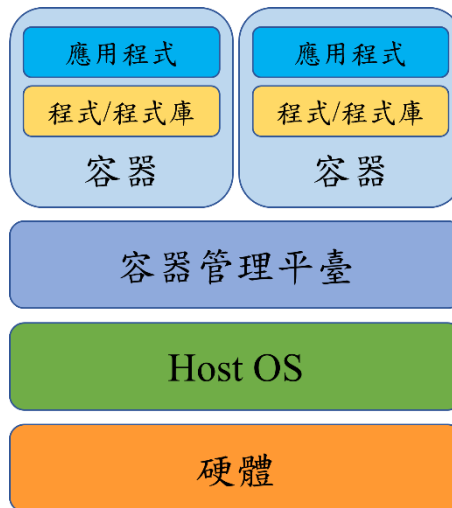


圖 9、容器技術架構圖

資料來源：本計畫整理

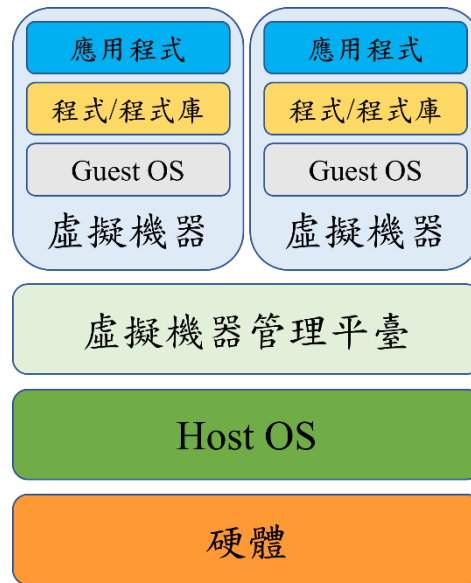


圖 10、虛擬機器技術架構圖

資料來源：本計畫整理

而容器與虛擬機器的虛擬化技術說明如下：

1. 容器

一種在概念上相似於虛擬機器，但在原理上略有不同的技術，其主要目的在於提供開發者用於測試應用程式的沙盒環境。開發者將想測試的應用程式與相依性資源 (Dependency) 封裝於容器進行測試。容器化與虛擬機器的相異之處在於，容器不會模擬系統底層的基礎架構，因此需耗費資源也相對較低，開發者能夠在容器內配置不同的資源，因為每個容器都獨立運行且彼此之間不會互相影響。

2. 虛擬機器

是一種體積龐大且耗能高的軟體套件。虛擬機器模擬底層的主機資源，將資源配置給上層的應用程式使用。在虛擬機器技術架構中有一層名為 Hypervisor 的平台，被用於管理硬體資源使用和配置，讓使用者能夠在作業系統上 (Host OS) 增加另一個作業系統 (Guest OS)，並且讓 2 種作業系統相互

協作。每個虛擬機器包含操作系統、應用程式、必要的二進位檔案和系統程式庫的完整副本，容量大約為 10 GB，因此虛擬機器啟動時間較為緩慢。

雖然容器和虛擬機器具有類似功能及優勢，但被用於處理不同面向的問題，虛擬機器主要功能是作業系統的虛擬化，容器主要功能是虛擬化應用程式和其相關的環境，因此容器相較於虛擬機器更容易攜帶，也更高效，如表 5。

表 5、容器技術及虛擬機器技術特性比較

功能	容器	虛擬機器
虛擬化的目標	應用系統	作業系統
啟動時間	短(幾秒)	久(幾分鐘)
映像檔大小	KB~MB	GB~TB
複製相同環境	快	慢
耗費資源	較少	較多
服務內容	多使用於微服務中	大型專案服務
系統支援量	上千個容器	幾 10 個虛擬機器
效能	快(接近傳統實體機)	較慢
資源用量	0~5%	5~15%
高可用性策略	備份、備援	動態調整

資訊來源：本計畫整理

而容器與虛擬機器的管理平臺介紹如下：

1. 容器管理平臺

當組織的 IT 管理人員使用容器技術時，只要透過 Docker 容器管理技術即可使用。然而，隨著組織使用容器數量逐漸變多，將增加 IT 管理人員工作負擔，也就需要有一個管理及調度眾多容器的工具平臺。在實務上每臺實體機器可運行多個 Docker 容器服務，當需要在機器上啟用多個 Docker 容器時，對於眾多容器管理該有妥善的處理。此時就

需所謂的容器管理平臺協助處理，使用戶能夠方便定義、部署、擴展和管理容器。目前坊間有各種容器調度管理工具，如 Docker Swarm、Kubernetes，以下針對此 2 項容器調度管理工具描述解析：

(1)Kubernetes：

Kubernetes 由谷歌公司(Google)發展，以 GO 語言進行開發，其前身是 Google 內部 Borg 叢集管理系統。在 2014 年 6 月對外發表，於 2015 年 7 月釋出 v1.0 後並交由雲端原生運算基金會持續開發維護。以往系統管理者如圖 11 所示需要各別管理不同主機內的容器，為確保所有容器服務正常，管理者需設置對應監控系統並手動重新部署有問題的環境，在管理上非常不易且繁雜。

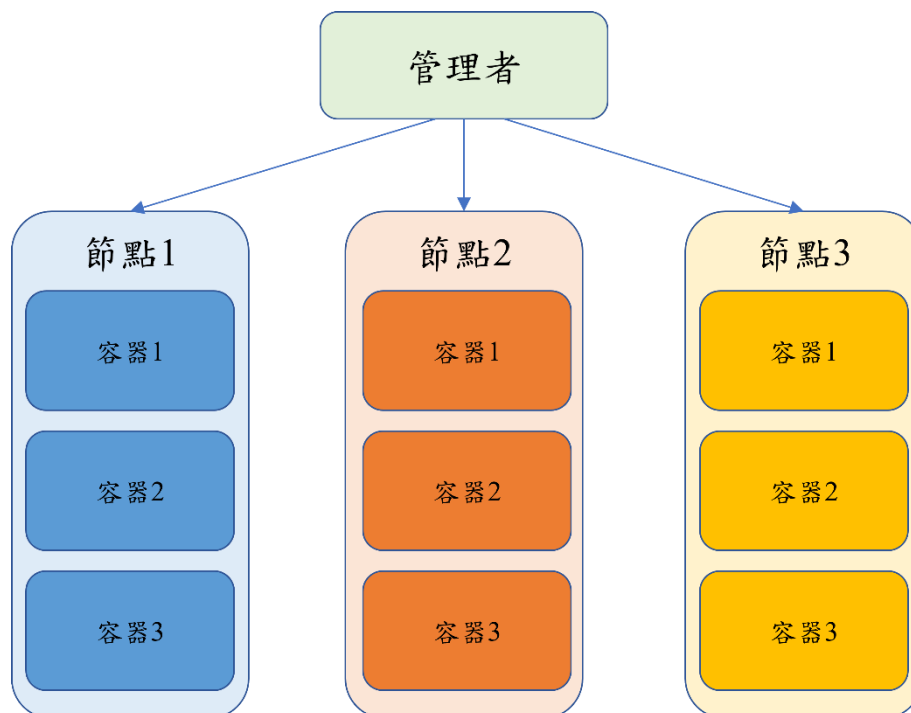


圖 11、傳統容器管理模式

資訊來源：本計畫整理



Pod 和容器在 Kubernetes 中代表不同概念，容器是一個獨立運行的軟體封裝，包含應用程式和其所有的相依性，如程式庫、執行環境等。容器技術讓應用程式可以在一個標準化的環境中打包，並在不同平臺和環境中運行。而 Pod 是 Kubernetes 基本調度和部署單位，是一個邏輯上相關的容器組合，可以是一組（一個或多個）容器，各容器共享一些特定的網路和儲存資源。而 Kubernetes 提供可彈性運行分散式系統的自動化管理架構，需要建立一個主管節點(Master Node)以集中式控管所有工作節點(Worker Node)，使得應用容器的部署、調度和管理更加方便有效進行如圖 12。從服務的自動部署、自動修復、負載平衡、權限控管到服務間的溝通與滾動式更新都可以透過 Kubernetes 達成，其中 Kubernetes 軟體特點整理如表 6。

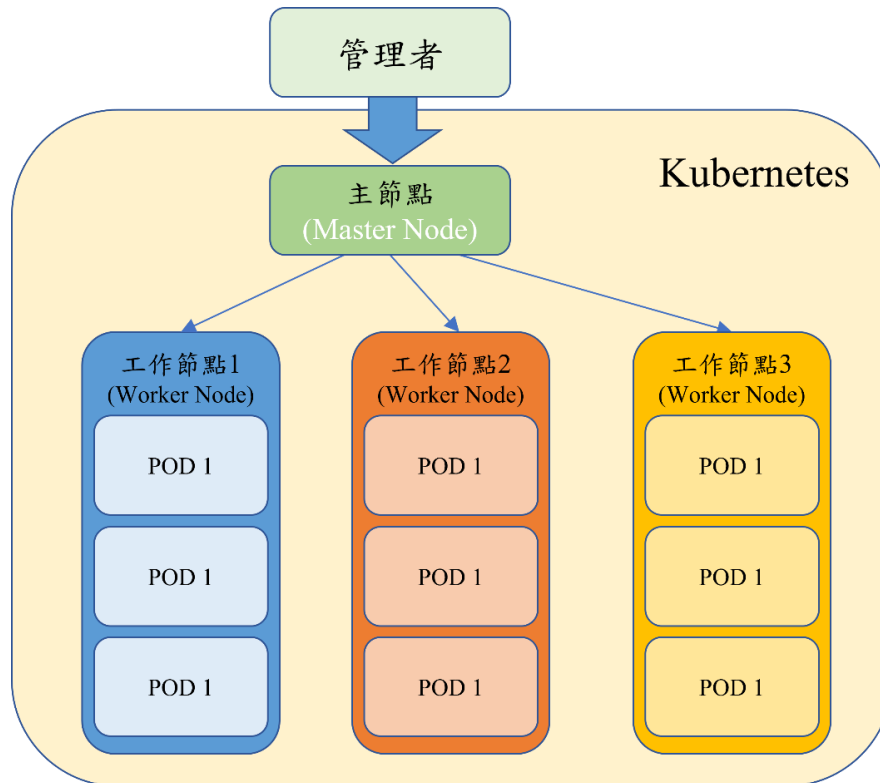


圖 12、Kubernetes 容器管理模式

資訊來源：本計畫整理

表 6、Kubernetes 容器管理平臺特點

特點	說明
容器管理	根據管理者設定的環境條件將其部署到集群中適當節點上。管理容器生命週期，即時監視容器的狀態，自動重新啟動失效的容器。
依負載擴展容器	根據應用程式的負載狀況自動擴展或縮減容器數量，執行動態調整資源的運用，自動化處理以維持系統高可用性、穩定服務和服務效能。
自我修復	可以自動偵測容器狀況，處理失效的容器。 Kubernetes 會自動關閉失效容器，然後重新啟動一個新容器，將工作負載轉移至新容器上，自動進行故障轉移，以確保應用程式連續運行。
服務發現	目的是使分散系統上的服務，能夠自動發現並確定彼此位置和通訊方式，以便進行正確連接和互動。

特點	說明
	Kubernetes 服務發現機制將負責查詢服務映射到相應的服務地址，並連結到正確目標之容器或應用程式，提供高彈性和可靠性。
設定與機密資料管理	Kubernetes 可以管理應用程式的設定，儲存管理敏感資料如密碼、金鑰，供給容器使用，並支援各種儲存解決方案。
安全性	Kubernetes 提供多層次安全機制，包括容器隔離、身分鑑別、授權和允許用戶定義准許或禁止 Pod 之間的通訊網路策略等。
多租戶支持	支持多租戶部署，使不同用戶或團隊可以在同一個集群中獨立運行和管理自己的應用程式。
擴展性和彈性	Kubernetes 架構具有高度擴展性，可以擴展到數百個或數千個節點集群，並支持彈性調整，可根據需要動態增加或減少節點數，以滿足不斷變化的工作負載。

資料來源：本計畫整理

(2) Docker Swarm：

在目前市場上主流容器管理平臺為前述的 Kubernetes，然而 Docker Swarm 擁有 Docker 原生技術與組態設定較為簡單的優勢，對於部分中小規模使用 Docker Swarm 相對簡單易用，並且與 Docker 容器技術緊密結合。Docker Swarm 仍然是市面上可見的選擇，在容器調度管理平臺的市場中仍占有一席之地，Docker Swarm 容器調度管理平臺特點如表 7：

表 7、Docker Swarm 容器調度管理平臺特點

特點	說明
叢集管理	Docker Swarm 架構上，將多個 Docker 主機組成一個叢集，實現容器的分散式管理和部署。用戶可以將主



特點	說明
	機加入 Swarm 叢集，並使用 Swarm 指令或 API 進行叢集管理和操作。
服務定義	服務是應用程式的邏輯組合，可以由一個或多個容器共同合作完成。用戶可以使用 Docker 指令或 Docker Compose 文件定義和設定容器服務，其中包含網路設定、磁碟掛載、資源配置等參數，Swarm 則會負責將服務的容器配置在叢集不同節點上。
服務發現和負載平衡	Swarm 有內建服務發現機制，會為每個服務配置一個唯一網域名稱系統(Domain Name System, DNS)，使用已建構的負載均衡演算法，請求分發到不同容器執行，並將使用者的服務請求工作負載平均配置至每個容器，藉以確保負載平衡和系統可用性。
容器管理及調度	Docker Swarm 提供基本功能的容器管理如容器啟動、停止、擴展和更新等，使用者可以通過命令列介面或 API 管理和操作各種容器服務。並依據使用者設定的規則和資源要求，考量節點上負載情況和容器限制條件，自動將容器調度調配至可用且適當的節點上，以優化容器調度和資源利用。
安全性	Swarm 提供必要的安控機制，包括通訊加密、存取控制和節點身分鑑別等。確保叢集內的溝通安全性，以防止未經授權的存取。
可擴展性	Swarm 可以根據需要加入或刪除節點來擴展叢集規模，因應負載需求變化，支援自動服務發現和容器調度，具有可擴展性。
滾動式更新	透過滾動式更新機制，管理人員可以簡易地更新不同版本容器映像檔，並且在發生問題時恢復到先前運作良好的版本。

資料來源：本計畫整理

Docker Swarm 和 Kubernetes 為最多人採用容器管理平臺，在管理容器化應用方面有一些相似之處，但是 Kubernetes 和 Docker Swarm 之間存在一些顯著的差異如表 8：

表 8、Kubernetes 和 Docker Swarm 比較

	Kubernetes	Docker Swarm
優點	• 大量開源社群支持 • 支援多種作業系統 • 支持和管理大規模的架構和複雜的工作負載 • 自動化和自愈能力 • 預設監控和強大的整合能力	• 使用較容易上手 • 與 Docker 相關工具緊密整合，無需再安裝新的命令列工具 • 自動負載平衡 • 已在 Docker 運行服務，不需進行更新設定
缺點	• 安裝過程較為複雜 • 需要安裝單獨的命令列工具 • 特定情況下，由於過於複雜，效率下降	• 功能有限 • 自動化能力較弱

資料來源：本計畫整理

總結來說，選擇容器管理平臺取決於應用服務具體需求、項目規模和複雜性。Docker Swarm 適合需要簡易入門操作容器管理的用戶，或對功能要求相對簡單的用戶。而 Kubernetes 適用於需要管理複雜部署使用情境和大規模工作負載的企業開發團組織。

2. 虛擬機器管理平臺

虛擬機器管理平臺是透過如 CPU、RAM、儲存和網路等硬體資源進行抽象化表現，以便在資源上運行多個虛擬機器，目前市面上常見的虛擬機器管理平臺如下：

(1) VMware vSphere：

而 vSphere 是由 VMware 公司所開發虛擬機器管理平臺，是一個集中管理和優化虛擬基礎架構的軟體解決方案，用以管理和操作虛擬機器，優化資源使用、實現高可用性和自動化管理。VMware vSphere 特點如表 9：

表 9、VMware vSphere 虛擬機器管理平臺特點

特點	說明
虛擬化	vSphere 為一個完整的虛擬機器管理平臺，可將實體伺服器轉換為虛擬機器，並在單個實體伺服器上運行多個虛擬機器，從而提高資源利用率和效能。
集中管理	vCenter Server 是 vSphere 的核心管理平臺，提供集中化界面，管理員透過此界面管理及監控多個主機和虛擬機器，管理員可以進行虛擬機器配置、資源配置、性能監控和故障排除等操作。
自動資源配置	可以根據資源需求和性能指標，動態地在主機之間遷移虛擬機器，實現資源平衡和性能優化。
高可用性(High Availability, HA)	vSphere 有提供高可用性功能，可以在主機故障時自動重新啟動虛擬機器。
容錯(Fault Tolerance, FT)	容錯功能可以創建虛擬機器的即時副本，實現無間斷的連續運行。
虛擬機器無中斷遷移	vSphere 可以無需中斷進行遷移正在運行中的虛擬機器。因應負載平衡、故障排除和資源調整等狀況，將虛擬機器從一個實體機器移動到另一個實體機器。
儲存管理	vSphere 支持多種儲存選項，包括本地儲存、網路儲存和儲存區域網路(Storage Area Network, SAN)儲存，在資料儲存功能提供儲存虛擬化和儲存管理功能。

特點	說明
安全性	vSphere 提供虛擬機器防火牆、虛擬機器加密和身分驗證機制等多項安全功能，並對客體作業系統提供防護。

資料來源：本計畫整理

就系統運作面向觀之，虛擬機器是虛擬化技術的實現，而 vSphere 是一個完整的虛擬機器管理平臺，用於管理和操作虛擬機器，可以創建、配置、監控和遷移虛擬機器，簡化管理人員複雜的操作，提供許多功能和工具優化虛擬化基礎架構的管理、效能以及安全性。

(2)VirtualBox：

VirtualBox 是一套免費的虛擬機器，最初由德國 InnoTek 軟體公司所開發，後由甲骨文公司(Oracle)收購並接手持續開發、維護到現在。它提供功能豐富的虛擬化環境，允許用戶在單個主機運行多個獨立的虛擬機器。VirtualBox 的主要特點如表 10：

表 10、VirtualBox 虛擬機器管理平臺特點

特點	說明
跨平臺支持	VirtualBox 可在多種主要作業系統上運行，包括 Windows、Mac、Linux、FreeBSD 和 Solaris 等，使用者可以在不同的作業系統上運行和測試應用程式，或者在一臺主機上創建多種不同作業系統的環境。
容易安裝、使用	VirtualBox 提供一個直觀的用戶界面，管理者能夠直覺地創建、配置和管理虛擬機器。
多機器管理	用戶可以管理和控制虛擬機器群集，並提供管理工具如虛擬機器的創建、複製、匯入(Import)、匯出(Export)、快照、網路設定和資源配置等。
硬體虛擬化	VirtualBox 利用如 Intel VT-x、AMD-V 和 Intel EPT 等硬體虛擬化技術，以實現高效和穩定的虛擬化性能，

特點	說明
	虛擬機器在主機上運行速度近乎在原生系統上的運作速度。
網路配置	VirtualBox 提供包括網路位址轉譯(Network Address Translation, NAT)、橋接、內部網路和僅主機(Host-only)等模式的網路配置選項。虛擬機器可以與主機及其他虛擬機器透過網路通訊，實現各種網路配置需求。
快照和回復	提供虛擬機器快照功能，可以儲存虛擬機器的狀態並保存為快照，並且可以依實際狀況回復到先前穩定的狀態，還原虛擬機器配置和內容。

資料來源：本計畫整理

VirtualBox 具備跨平臺且容易上手應用的虛擬機器管理平臺，現仍持續維護各種功能和工具，比較適合個人和小型組織用來創建和管理虛擬機器，在開發、測試和教育等領域中廣泛被應用。

(3)Microsoft Hyper-V：

Hyper-V 舊稱 Windows Server Virtualization，是微軟（Microsoft）的虛擬機器管理程式，可以在執行 x86-64 位元的 Windows 上建立虛擬機器。從 Windows 8 開始，Hyper-V 取代 Windows Virtual PC 作為 Windows 用戶端版本的硬體虛擬化元件。可以組態執行 Hyper-V 的伺服器電腦，能夠將單個虛擬機器公開到一個或多個網路。可以在電腦上新增多部虛擬機器，視實際需求安裝如 Windows、Linux 等作業系統，已安裝好作業系統的虛擬機器上，可隨意修改測試或安裝軟體，也不會影響電腦的運作。Hyper-V 是一套免費軟體，

只要是 Windows 10 或 Windows 11 的專業版，就可以開啟使用。Hyper-V 特點如表 11：

表 11、Microsoft Hyper-V 虛擬機器管理平臺特點

特點	說明
原生支援 Windows	Hyper-V 是一個基於 Windows 作業系統而設計的虛擬機器管理平臺，能夠與 Windows 環境無縫整合。支援包括不同版本的 Windows Server 和 Windows 作業系統的虛擬機器。
Type-1 Hypervisor	這表示它直接運行在硬體上，而不需要在作業系統之上運行。Hyper-V 即此類型的虛擬化，意味著可提供較高效的虛擬化性能和低延遲。
功能多樣	Hyper-V 提供包括動態 RAM 管理及調整、快照、複製等功能和工具，方便管理者能夠靈活管理和配置虛擬機器。
多用戶支援	Hyper-V 允許在同一個實體伺服器上運行多個獨立的虛擬環境，讓不同用戶共享同一個實體基礎設施，在各應用服務同時運行時，彼此之間仍保持隔離。
網路虛擬化	Hyper-V 提供網路虛擬化功能，包括虛擬交換器、虛擬區域網路等，提供用戶管理虛擬網路環境功能。
硬體支援	Hyper-V 支援多種硬體架構，包括 x86 和 x86-64，能夠運行在各種硬體平臺上，支援彈性化的部署。

資料來源：本計畫整理

Hyper-V 是一個專為 Windows 環境而設計的虛擬機器管理平臺，提供多樣的功能和工具，方便用戶管理虛擬化。Hyper-V 在伺服器虛擬化、雲端運算和桌面虛擬化等應用都提供相對應的虛擬化解決方案。

(4)Xen：

Xen 虛擬機器管理平臺是基於 X86 硬體由 Xen Project 開發的虛擬機器監督器(Virtual Machine Hypervisor)，

以 GNU 通用公眾授權條款 (GNU General Public License, GNU GPL) 授權發布的自由軟體，其發展目的期可提供效能佳，和支援不同作業系統同時運作，且同時運作的系統互相獨立，能夠在一臺電腦上執行多達 128 個獨立功能的作業系統。

與一般可直接使用作業系統如圖 13 所謂的全虛擬化技術架構不同，Xen 要求虛擬機器使用用戶端作業系統需要經過適當的修改，如圖 14 的 Modified Guest OS，達成半虛擬化技術，以達到高效能的表現。一般全虛擬化技術約會有 20% 的效能損耗；而 Xen 的半虛擬化技術在典型的情況下大約是損失 2% 效能，最糟的情況下則會有 8% 效能耗損。此外，Xen 亦有全虛擬化模式，但是僅限於 x86 平臺上，允許 Xen 虛擬機器執行未經修改的作業系統。Xen 的特點如表 12：

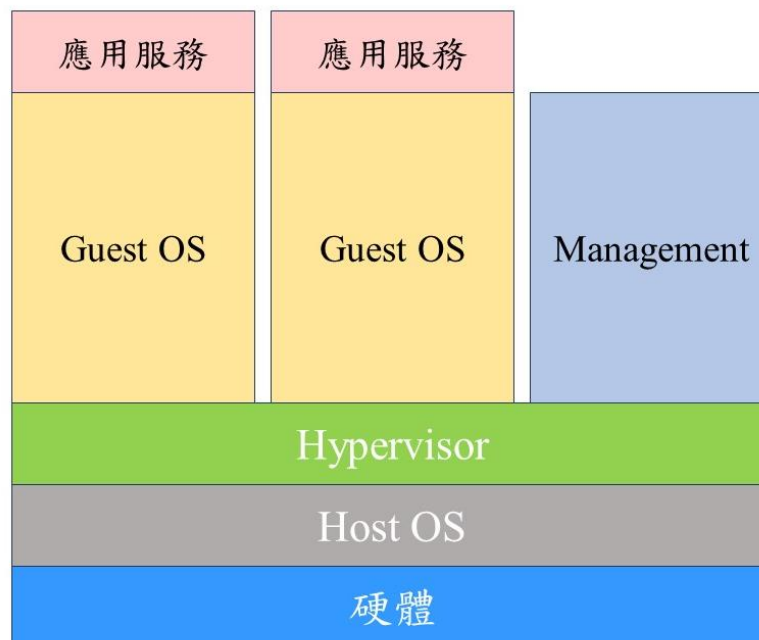


圖 13、全虛擬化技術

資料來源：本計畫整理

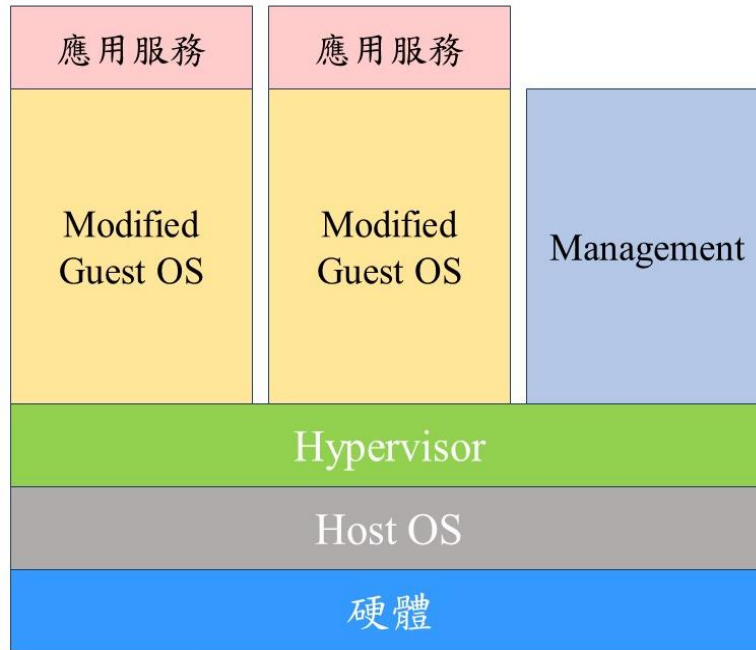


圖 14、半虛擬化技術

資料來源：本計畫整理

表 12、Xen 虛擬機器管理平臺特點

特點	說明
輕量級 Hypervisor 架構	Xen 使用一個輕量級 Hypervisor 架構，直接運行實際硬體上，可直接配置和管理硬體資源，提供高效能和低延遲的虛擬化解決方案。
完全虛擬化和半虛擬化	Xen 支援完全虛擬化和半虛擬化，如圖 13 所示完全虛擬化可以在虛擬機器中運行原始未修改的作業系統。而圖 14 所示半虛擬化，則要求作業系統必須進行修改以提高效能。
高性能	Xen 的 Hypervisor 架構和半虛擬化技術讓虛擬機器可以獲得接近原生系統的效能。此外，Xen 提供優化 I/O 路徑、高效的網路和儲存性能。
可靠性和安全性	Xen 提供強大的安全性和隔離機制，讓虛擬機器之間嚴格隔離，同時具備故障隔離和恢復機制，當一個虛擬機器失效時，仍可讓其他虛擬機器持續運行。

特點	說明
跨平臺支援	Xen 可以在多種硬體架構和作業系統上運行，包括 x86、ARM、PowerPC 等硬體架構，客端作業系統則有支援 Linux、Windows、FreeBSD、OpenBSD 等作業系統，具有廣泛相容性的虛擬化解決方案。

資料來源：本計畫整理

Xen 包括伺服器虛擬化、雲端運算、桌面虛擬化等使用情境被廣泛應用，也被許多組織和企業信賴及使用。表 13 為前述 4 項虛擬機器管理平臺的特點比較：

表 13、虛擬機器管理平臺特點比較

	VMware	VirtualBox	Hyper-V	Xen
適用對象	企業環境	個人使用	企業環境	大型數據中心
跨平臺支援	Windows、 Mac、 Linux、 FreeBSD、 Solaris	Windows、 Mac、 Linux、 FreeBSD、 Solaris	Windows	Linux、 Windows、 FreeBSD、 OpenBSD
效能	普通	普通	普通	高
Guset OS	不需修改	不需修改	不需修改	需修改
購買成本	需要	免費	免費	免費
網路支援	佳	普通	佳	佳
軟體支援	企業	社群	企業	社群

資料來源：本計畫整理

二、Cloud-Native 技術的相關特性

Cloud-Native 應用程式的設計和建置，其目的期望能夠充分利用雲端所提供的規模、彈性、復甦力和彈性，建構和部署快速、靈活、可靠地運行在雲端環境中的應用服務。以下是 Cloud-Native 的優點和缺點：

(一)優點

- 1.資源調度彈性化：Cloud-Native 應用程式可以根據運作狀況增減運算資源，從而實現系統彈性的資源運用。例如能夠根據流量、負載、實體機的情況動態調整資源使用，以滿足不斷變化的實際狀況需求。
- 2.高可用性容錯性：架構於雲端環境所提供的高可用性功能的特性，Cloud-Native 應用程式可以實現高可用性。當一個組件或節點發生故障時，應用程式可以自動/手動轉移到其他可用的資源上，以確保服務的連續性。
- 3.靈活的部署環境：Cloud-Native 應用服務採用虛擬化的部署方式，讓應用服務的部署更簡單和靈活。應用程式可以在不同的雲端環境中運行，實現跨平臺和跨雲端提供商的高度移植性。

(二)缺點

- 1.學習曲線陡峭：Cloud-Native 技術涉及到眾多不同的工具、框架和概念，對開發團隊來說需要一定的學習和適應時間。
- 2.較複雜：虛擬化元件管理工具、微服務架構和分散式系統的設計與傳統單機的應用服務有很大的差異，較不直覺需要深入理解和掌握，增加複雜性。
- 3.雲端基礎設施依賴：Cloud-Native 應用服務效能及運行與雲端基礎設施和服務相關，增加對雲端服務供應商(Cloud Service Provider, CSP)依賴。應用服務的穩定性和性能受到雲端服務的直接影響，如果雲端服務發生故障或有限制，可能會對應用服務產生影響。
- 4.安全及隱私的挑戰：雲端環境的與傳統單機式作法相較下更較複雜也更為開放，相對應的帶來一些安全性挑戰。虛擬機器及容器的安全性、網路傳輸的安全、資料的儲存、資料隱

私和合規性等議題都需要特別關注，需要採取適當的安全措施來保護資料和應用程式。

綜上所述，Cloud-Native 技術具有許多優點，但也需要克服學習曲線、複雜性和安全等挑戰。對於組織和開發團隊來說，了解優點和缺點、權衡實際需求、擁有的資源和永續服務等條件下，決定是否需要採用 Cloud-Native 技術，並選擇對應適當的開發工具，是很重要的一步抉擇。

三、AI-Native 架構、運作、特徵說明

(一)6G 網路 AI-Native 之必要性及效益

AI-Native 被業界認為是未來 6G 行動系統的核心架構特徵之一。AI 科技其相關的數學理論基礎、模型演算法、處理手段等都有突飛猛進的進展，在更緊密深入融合到未來 6G 系統架構、網路元件和作業流程之中，且基於電信基礎設施普及之現實優勢，將會更加彰顯出 AI 效能提升和價值，協助實現未來 6G 無線網路的願景實現。

(二)AI 在 5G 中的應用現況

目前業界對於 ML 和深度學習(Deep Learning, DL)等 AI 的討論及應用發展正方興未艾，但是與行動通訊系統的結合應用，雖於 5G 的行動通訊系統發展就已經在討論，已確立朝向 Cloud-Native，和軟體定義網路(Software Defined Networking, SDN)、服務虛擬化方向演進的趨勢。但 5G 在設計之初，以當時環境背景並未充分地考慮應用 AI 強化其相關能力服務，例如：如何使用 AI 技術去優化各種通訊機制。伴隨著近日來 AI 功能和應用的長足進展且彰顯 AI 未來各面向的價值，5G 在既定的系統架構和協議體系中，在核心網引入網路數據分析功能(Network Data Analytics Function, NWDAF)和各式各樣模組疊加、外掛上各種 AI 功能，進一步增強優化系統自身各方面的性能和對外服務能力。每個疊加的 AI 功能

模型，基本都是針對特定的通訊類問題提出解決方案，以提升 5G 系統性能、優化無線傳輸效率和簡化網路管理控制等目的。

(三)6G 下 AI-Native 機制的效益

業界普遍認為 AI-Native 將成為未來 6G 行動新系統的核心特徵之一，6G 行動系統從架構設計之初就已充分考慮如何和 AI 深度結合。5G 通過 AI 功能疊加、修補程式、外掛等方式的外顯式結合應用，而非原生於整體系統有所區別，這樣 AI-Native 的特性，不只是將 AI 作為優化工具的考量，對 6G 新系統設計亦會帶來種種的挑戰。

未來行動網路的演進，網路管理維運需要從降低成本增強效益的局部智慧化，邁進點到點的網路智慧自治。但是，現有網路 AI 的研發，普遍採用修補程式、外掛、疊加等方式進行，缺乏統一的系統框架。大部分 AI 模型缺乏驗證效果，AI 模型效果驗證只能在事後進行，無法實現高水平的網路自治、AI 模型效果預驗證、線上評估。此外，AI 模型訓練需要大量的樣本資料，而集中式蒐集資料困難，導致網路傳輸負載變大，AI 模型更新的週期較長，訓練負載較大、收斂慢、AI 模型泛化性差等。因此 6G 新系統需要進一步改善 AI 模型的訓練和應用性能，提升網路自治水平。面向各個行業的用戶，協助各行各業朝向智慧化轉型，探索新的智慧化商業模式，提供 6G 新場景和新能力都是內生智慧的重要驅動力。在保護垂直行業資料隱私、資料不出區域的前提下，6G 系統需能提供分散式、區域性運算資源、平臺和服務，實現「隨時隨地」智慧化能力依照需要靈活提供運算能量，較傳統雲端 AI 服務業者，在網路中對外提供智慧服務，深入融合行業智慧，支援更高的即時性、隱私性、性能更優的智慧化運算能力和服務，建立以資料為核心應用，創造新的市場價值。

AI 原生無線介面(AI-Native Air Interface, AI-AI)可以使用 AI 技術來優化和增強無線訊號傳輸和接收的介面，以適應不同的無線電環境、硬體、資料和應用程式。與傳統的無線通訊系統會事先定義通訊協定和設計好的訊號處理演算法，AI-AI 的概念則是分析大量的無線訊號資料，自動優化調整訊號處理參數，以提高傳輸效果。

另外，AI-Native 實現大規模智慧分散式協同服務，極大化網路中通訊與運算能量的效用，對於新興的 FL 機制更有推波助瀾的效果，促進實現跨領域、跨行業的智慧融合和數智共享。

AI-Native 深度融合 AI、ML 等技術，即時對無線環境、資源、干擾、業務和用戶等多維特性的深度挖掘和探索，顯著提升無線網路高效性、可靠性、即時性，實現網路的自主運行和自我演進。在重要的研究課題網路安全上，AI-Native 可促進實現網路的安全可信，系統可以具備自我檢測和主動防禦各種潛在的攻擊和威脅等。

(四)AI-Native 6G 必要性

AI 要與 6G 行動通訊成功的結合，須了解網路智慧化的可行性，以下從 AI 3 要素的角度(運算能量、AI 模型及資料)，分析未來 6G 行動通訊系統 AI-Native 深度融合的可行性：

1.運算能量

由於延遲、可靠性、資料安全及隱私保護等方面的要求，未來 6G 時代，資料的連接和運算可能進一步融合，例如：出現專為連結 AI 運算的基礎設施，可以為 AI-Native 的發生提供優化運算服務基礎。

2.AI 運算及模型

目前的做法會將各種資料集中到雲端，在雲端進行集中式 AI 處理的方式，此處理模式確有其優勢，但在資料隱私、運算耗能、通訊延遲等方面，一直存在其不足之處。如果未來 6G 行動通訊系統能做到將 AI 運算及模型和運算能量融

合到網路中，只要資料和任務存在哪裡，可以就地以 AI 技術進行的智慧處理，將成為一種更有效益的替代選項。因此，AI 運算及模型將由於資料和運算能量同時被下沉到網路邊緣(例如：邊緣節點、無線基站)來執行和維護。

3. 資料

目前通訊網路主要是資料傳輸的管道，除了行動通訊網路管理營運資料，不會主動產生和處理與業務不相關的資料。到 6G 時代，由於各種感知技術、行業數位化、邊緣運算素環境因等趨於成熟，6G 行動網路本身就是巨大的無線感測器網路，預期將具備主動產生和處理巨量不同結構資料的能力，為 AI-Native 6G 融合設計提供資料服務必要性相關的需求，例如：大量訓練樣本的採集和預處理等。

AI-Native 將更強化 AI 相關資源(包含 AI 運算能量、AI 運算及模型、資料)和 6G 行動通訊系統之間的整合，從而 6G 行動通訊系統內各種資源的組合使用率、利用效能、綜合效能等方面會更加優化，進而提供更高統成本和應用服務之間的性價比，一般消費者也能享受到更容易取得、更廉價的智慧應用服務。相較於目前常見的集中式架構雲端 AI 服務和邊緣運算的節點工作模式，AI-Native 模式使得 AI 資源能夠更廣泛、均衡地、更靈活依照實際需求部署在 6G 系統基礎設施之中，AI 的運算資源將更接近資料源、任務源和終端用戶，且更能高效適應無線網路的動態狀況(例如：用戶環境和通道變化，網路拓撲和資源更新等)，因此 6G 系統將可以針對用戶的動態環境進行快速、即時而精準的優化，進行趨勢預測提供適合網路環境的策略調整。

以 FL 為代表的分散式 AI 機器訓練模式下為例，此類不同於雲端集中化的 AI-Native 運作模式，將提供用戶資料更強的隱私保

護，並可分攤資料管理和 AI 運算的負載，進一步強化網路安全自治。

未來 6G 系統若可針對「資料」和「智慧面」等邏輯功能提供專門設計，進行更高效、靈活且強健的資料傳輸及共享，因此會帶來更低的傳輸延遲，更少的傳輸資源消耗以及系統耗能。

另一層面的思考，若是 6G 無線網路標準對於 AI-Native 技術完成標準化，可促進廠家之間的通訊、運算、AI 智慧設備、功能模型和 AI 處理流程整合，甚至帶來未來新型態商業模式。將進一步促進更多的廠商共同建構廣泛、可信賴的 AI 智慧資源能力服務平臺，從而實現在 6G 環境下 AI 服務及 AI 提供無所不在的願景。

(五)6G 下 AI-Native 的技術需求

預期 6G 無線通訊系統將會是深度融合「通訊」、「感知」、「運算」、「智慧」和「儲存」等方面更強大的能力，可以建構出較目前 5G 的系統下更強的技術特徵及效能，同時可以支援服務提供廠商、協力廠商及終端使用者更強的綜合業務、服務和應用。因此 6G 系統的特徵包含強大的無線通訊傳輸管道，龐大的分散式傳感網路、普遍存在運算能量和 AI 智慧服務的綜合體。AI-Native 與 6G 特徵息息相關，後續針對「運算能量」、「演算法」和「資料」3 大主要方面闡述 AI-Native 6G 在能力方面上的需求。

1.運算能量需求

6G 上強大的運算能力是有別於以往無線通訊系統的現重要特徵，是支持資料處理能力和服務的堅實基礎。現階段大數據、AI 等技術的高速發展，持續爆量產生資料，也因應需求讓 AI 演算法複雜度不斷提高，從而帶來對運算資源相關的需求的快速提升。對於運算資源的發現、感知、度量、調度利用也會成為未來行動網路發展的重要功能特徵。

(1) 依據需求調度運算資源：

6G 無線通訊系統結合雲端、霧、邊緣等運算資源，並且可透過 AI 進行系統優化的控管，還可透過堅實、強大的網路傳遞訊息，實現更廣泛的運算資源的管控和依實際需求動態調度，有效調度分散的運算資源，以達到綜合效能和資源使用最優化。

(2) 運算資源發現能力：

6G 無線通訊系統涉及雲端、霧運算、邊緣運算等多個面向運算資源的互動。運算資源的運算能量能和覆蓋範圍各有差異，6G 無線網路需具備運算資源的發現和註冊能力，以控制、提供不同需求的運算資源請求，例如支援即時的感測資料處理、控制執行等功能。

(3) 運算資源感知能力：

所謂對於運算資源的感知是系統對運算資源和運算資源服務的部署位置、即時狀態、負載狀況、業務需求的感知。典型的需求是簡單的資料感知、收集和運算資源服務需求資訊的存取和分析。未來 6G 的環境下各種資料會爆炸是成長以及需要更強大運算能力處理，運算資源的感知能力需要因應環境改變，需要更有智慧，實現更有效率的資料處理、資訊存取，提供座位分析決策的基礎。可以應用到環境監測、交通管理、城市治理等應用場景。

(4) 服務需求：

基於 AI 所產生的業務及服務才是彰顯對用戶和客戶有價值的要點。未來，6G 無線通訊系統所服務的對象從大致可分為個人、家庭、企業、行業及社會等；因

應每個不同的服務對象，對 6G 的 AI-Native 所提供的業務和服務的需求都會有所差異。

(5) 運算資源服務需求：

未來 6G 系統需要整合內部和外部的運算資源，實現系統運算資源開放共享和智慧 AI 服務，需要同時考量網路和運算的融合需求，發展多層運算網路融合合作的網路架構。其目標是，系統可以感知並控制運算服務，而用戶無需關心運算資源狀態；並且可彈性、動態地部署、調度運算資源到有需求的服務上。

另外，6G 系統運算資源服務至少要能夠支援下列服務類型：

(1) 延遲敏感型服務：

透過 6G 系統的智慧感知和決策，即時為用戶 AI 服務提供充足的運算資源，加速傳輸和運算效能，從而達到較短時延。應用場景例如：沉浸式虛擬現實 XR。

(2) 耗能敏感型服務：

6G 系統能夠將高耗能型 AI 運算任務遷移到其他較無耗能資源進行運算工作，避免本地運算帶來耗能。應用場景例如：搶險救援、農業數位孿生等。

(3) 隱私敏感型服務：

用戶無需上傳私密資料經過複雜的核心網路到達雲端資料中心，只需通過 6G 系統運算資源調度和配置進行可靠的高隱私運算。應用場景例如：普惠金融、資料孤島等。

(4) 服務體驗敏感型任務：

多層運算網融合具備與用戶距離較近的優勢，可通過系統智慧感知準確地預測和判斷出用戶的運算行為和

需求，能夠及早調度運算資源，提供更即時有效的運算服務。應用場景例如：XR、感官互聯等。

2.AI 運算及模型需求

6G 新網路對外提供的 AI 運算及模型至少需要支持以下特性：

(1)標準化 AI 運算及模型描述和儲存管理：

6G 系統需要定義出標準化的 AI 運算及模型管理框架，在相同架構下用標準化的描述語言定義演算法模型和其相關服務。

(2)AI 運算及模型分類索引和服務介面：

系統應定義 AI 運算及模型的分類和索引，使用者通過標準化的服務介面使用 AI 運算服務，提供各種索引方式。

(3)AI 運算及模型認證：

AI 運算及模型必須確認其性能、安全性、資料隱私性，經過認證後才能提供做為 6G 環境中 AI-Native 可使用運算方法。

(4)重複使用 AI 模型：

如果對每一個的 AI 請求都獨立配置演算法及模型，將是系統很大的負擔，所以系統應支援重複已存在或已訓練好的 AI 模型，來因應類似的應用情境，減輕系統 AI 運算的負擔。

3.資料服務需求

6G 行動通訊系統在初步發想時期就已普遍有與 AI 和大數據技術融合的共識。6G 網路應可支持獨立的資料面功能，透過建資料服務框架，在確保資訊安全和隱私的基礎上，完備 AI-Native 技術的必要根基，以滿足用戶資料蒐集、ML、

AI 服務和應用等一系列動作 AI-Native 服務的需求，進而提供更快的傳輸速率和更可靠的傳輸鏈連結，滿足未來更多種應用服務類型、數量增加和更嚴苛服務品質的需求。

要達成這些目標就需要強化處理巨量資料流程中各環節的處理能力，比如在資料蒐集、標注和特徵提取等方面進一步提升。為提供 ML 和 DL 應用的模型中獲得好結果，資料的格式也必須以適當的方式格式化和存放。

(六)6G 下 AI-Native 架構

基於前述各個 AI 資料功能，系統還要依照客戶需求提供各類 AI 資料服務，服務內容包含 AI 資料本身，及各個 AI 資料集所對應的資料服務項目。透過合理且審慎規劃的網路架構下儲存功能和資料傳輸方式，確保 AI 資料在網路中高可靠、低延遲的傳輸，滿足 AI 演算法模型訓練，驗證和推理決策等過程的需求。

1. 運算能量架構

近年來，AI 技術呈現跳躍式的進步，應用服務逐漸趨向智慧和複雜化發展。6G 系統所提出新型態應用場景如沉浸式雲端 XR、智慧城市等，對傳統的行動通訊網路也提出諸多挑戰，預期將會有巨量的終端設備連接上網路，導致網路膨脹。傳統行動網路上，運算和通訊的運作各自獨立互不相干，兩者之間並不存在有效管理和融合的機制；未來 6G 需要更迅速敏捷部署新的業務，而傳統網路的運作迭代升級耗時耗力。

基於各種新的需求，6G 行動網路在建構階段，除了要考量以往傳統的系統維運問題，還應該考慮到各種資源的應用，如更充分的利用邊緣算力資源。可以期待的是，未來 6G 網路應當具備管理各個服務節點各種訊息，包括運算資源資訊、資料儲存資訊、AI 演算法及模型訊息等，整合網路訊息

提供用戶最佳的各種資源配置和網路連接解決方案，實現 6G 行動網路對於運算、通訊及 AI 相關資源優化使用能力。

未來 6G 行動網路預計是個由雲端、網路、邊緣運算以及智慧終端混合，運算資源與網路資源融合在一起的多層次「運算網路融合」，所謂新形態網路系統，較傳統網路以通訊為主更加強化運算相關的功能，6G 行動網路會將運算、通訊、控制、儲存整合提供更強化服務的新型架構。

運算網路融合系統是一個多層網路，其中運算和通訊的節點可以提供原生運算資源，可以最佳化運算和通訊能力。運算網路融合系統可支援各種應用，除了透過調度運算資源進行合理地配置，另一方面提供網路運算能力和通訊服務管理，如處理和轉發從雲端到邊緣層的控制指令等。

多層運算網路融合系統架構，可使能夠提供出運算資源與通訊融合的各種創新服務和應用。運算資源可以由網路中心/高層往更鄰近使用者的位置，以獲得以下效益：

- (1)最小化延遲：有些應用要在一定時間限制下驅動適當地處理動作，對時間非常敏感。在本地或靠近資料源的地方分析並做出快速決策，可以減少控制所產生延遲。
- (2)提高系統可靠性：感測器資訊透過網路會傳遞至遠處的雲端的可能被破壞，因此可以視應用服務性質，以本地處理當作備援選項，或完全使用本地處理的模式。
- (3)減緩隱私洩漏風險：如用戶個資，或是法規要求的敏感資料需要審慎維護其隱私性，即使雲端服務提供商一般被認為是可信的，但用戶無法知曉和控制這些敏感資料實際存放地點、誰可以存取使用。基本上，本

地網路元件和邊緣節點則是在本地人員的控制之下，
可以提供使用者較佳的信任。

- (4)節省頻寬：在本地端先處理完資料，再將處理結果資料傳送到雲端，可以顯著減少上行傳輸頻寬的消耗。

2.AI 演算法及模型架構

針對 AI-Native 6G 的演算法及模型架構的設計，應當充分考慮通訊網路不同特性的需求和影響，從 6G 系統架構的觀點來規劃 AI 演算法及模型管理。

6G 的 AI 演算法及模型架構應當至少滿足如下需求：

- (1)穩定性：電信級行動網路需要非常穩定地運行，因此對 AI 演算法及模型運行和維護的穩定性也會有更高的需求，需要具備穩定的結構與系統化設計，並應考量有更強的容錯能力。
- (2)實時可管可控：AI-NativeI 演算法架構需提供網路訊息智慧化的即時監控、管理與控制。AI 演算法及模型管理架構在設計時，應充分考慮電信網路即時性需求。
- (3)安全與隱私保護：AI 演算法及模型架構應當支援不同運算資源、設備之間資訊傳遞的安全和隱私保護。
- (4)混合層級設計：行動通訊網路是一間據分散式和中心化的多重混合式結構。部署 AI 演算法及模型理應要考量支援多層靈活混合式部署和運行，並從如何提供資訊優化電信網路運作考量。
- (5)運算與網路一體：運算與網路兩者一體存在，且會協同運作將會是未來 6G 新網路的重要特性之一。因此，AI 演算法及模型應當充分考量此網路特性，在架構設計上體現出運算資源與網路深度結合的需求。

- (6)可自我演進性：AI 演算法及模架構應具備可演進性，要能因應網路技術發展和應用服務的變換持續改進，貼合實際網路應用需求，甚至有更好的 AI 演算法及模型也進行適當調整。

3.資料架構

資料管理的架構對於 6G 網路架構至關重要，它主體現在對各資料生命週期相關功能實體的組織相關性。

圖 15 資料管理建議架構說明 6G 資料管理可能存在各功能實體，系統架構設計者可以因應其實際需求，調整架構以適應現實環境的需求：

- (1)資料開放功能：用於向「應用服務功能」開放 6G 網路資料相關服務。可根據「應用服務功能」提供應用服務需求或服務水準協議(Service Level Agreement, SLA)規範將 6G 網路資料進行去識別化、聚合等處理，作為資料服務提供給外部廠商或內部應用。
- (2)資料蒐集功能：用於收集 6G 系統內的網路、業務和終端等資料，供「資料分析功能」實體使用。
- (3)資料分析功能：用於「資料蒐集功能」收集的資料，進行 AI/ML 模型訓練，進而利用 AI/ML 演算法得到和網路、業務和終端相關分析結果資訊。
- (4)資料安全管理：用於針對 AI/ML 相關資料進行隱私保護和安全管控。須提供資料擁有者對資料處理的授權相關權力，如許可、修改和撤銷的權力，以此為基礎可以控制系統用戶對於資料管理使用和處理。
- (5)資料儲存功：用於儲存 AI/ML 相關資料。

(6)資料資源編排功能：用於配置、調度、移除 AI/ML 資料處理相關資源。本身也可基於 AI 演算法，對資料處理資源進行動態智慧的編排和管理。

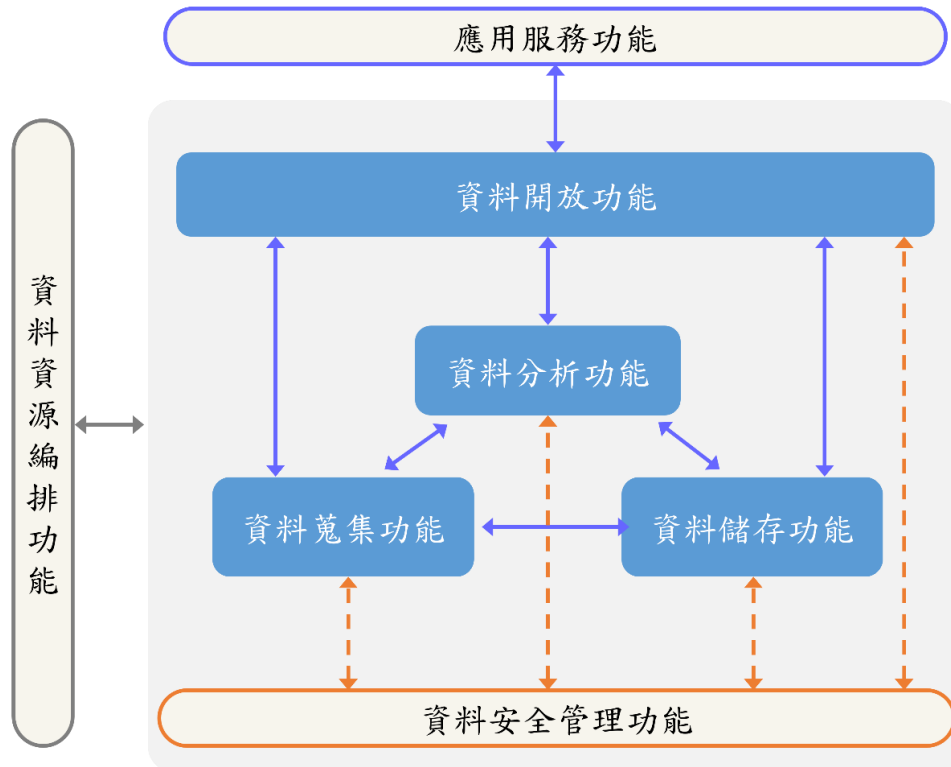


圖 15、6G 資料管理架建構議

資料來源：請參閱附錄-參考資料^{2.12}

基本上 6G 行動通訊系統下 AI-Native 的實現，在其能力、服務、架構技術需求方面都會涉及到「運算能量」、「AI 演算法及模型」和「資料」3 要素方面，如圖 16。本計畫整理出相關的技術考量，做為未來能支援可差異化、客製化的 AI 能力和服務應用，以支撐對應的 AI 商業模式新應用。

2.12 6G-ANA (2022). 6G 网络原生 AI 技术需求白皮书. (2022). Retrieved from <http://www.6g-ana.com/upload/file/20220523/6378893017730497434706068.pdf>

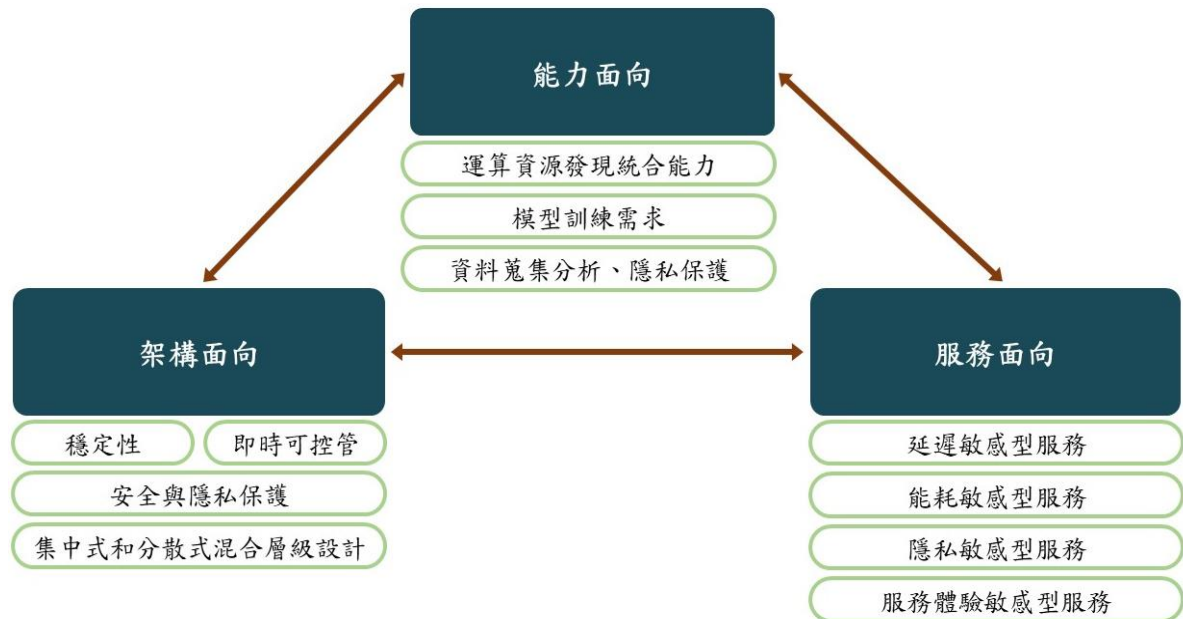


圖 16、6G 之 AI-Native 融合架構考量

資料來源：本計畫整理

應用服務是一個通訊系統可以長久運作的基礎，考量 6G 之 AI-Native 3 個要素面向，以延遲敏感型、能耗敏感型等類型服務為主要觀察點，對於其他能力、架構 2 個要素需求的考量重點，整理如圖 17 所示。例如以能耗敏感型的服務，不適合在其附近進行運算，所以需要採用線上或離線訓練方式進行處理，其資料蒐集避免以集中式減少負擔，可以盡量採用分散式方式，所以其資料管理上的要求會較高。在網路架構上，比較會以降低能耗為基礎思考，比較趨於平衡型式的建議，意即依應用服務實際的運作狀況，採用符合需求的網路架構。

		能力面向					
		運算資源發現 及統合	模型訓練 需求	資料蒐集 分析管理	其他能力		
服務面向	延遲敏感型	霧運算、 邊緣運算	線上訓練	資料蒐集功能	演算法指標需求：高 依需求調度運算資源能力： 考量網路通訊及運算資源， 穩定服務延遲	即時可控管	
	能耗敏感型	雲運算	離線訓練	資料管理功能	運算能力統一度量能力： 具備平行運算能力 依需求調度運算資源能力： 可分散至其他低能耗節點 運算，避免集中	集中式和分散式 混合層級設計	
	隱私敏感型	邊緣運算	聯合訓練	資料儲存及 管理功能	資料隱私安全保護 能力	安全與隱私 保護	
	服務體驗 敏感型	霧運算、 邊緣運算	線上訓練	資料蒐集功能	依需求調度運算資 源能力	穩定性	
		能力面向					
		運算資源發現 及統合	模型訓練 需求	資料蒐集 分析管理	其他能力		
		霧運算、 邊緣運算	線上訓練	資料蒐集功能	演算法指標需求：高 依需求調度運算資源能力： 考量網路通訊及運算資源， 穩定服務延遲	即時可控管	
		雲運算	離線訓練	資料管理功能	運算能力統一度量能力： 具備平行運算能力 依需求調度運算資源能力： 可分散至其他低能耗節點 運算，避免集中	集中式和分散式 混合層級設計	
		邊緣運算	聯合訓練	資料儲存及 管理功能	資料隱私安全保護 能力	安全與隱私 保護	
		霧運算、 邊緣運算	線上訓練	資料蒐集功能	依需求調度運算資 源能力	穩定性	
		能力面向					
		運算資源發現 及統合	模型訓練 需求	資料蒐集 分析管理	其他能力		
		霧運算、 邊緣運算	線上訓練	資料蒐集功能	演算法指標需求：高 依需求調度運算資源能力： 考量網路通訊及運算資源， 穩定服務延遲	即時可控管	
		雲運算	離線訓練	資料管理功能	運算能力統一度量能力： 具備平行運算能力 依需求調度運算資源能力： 可分散至其他低能耗節點 運算，避免集中	集中式和分散式 混合層級設計	
		邊緣運算	聯合訓練	資料儲存及 管理功能	資料隱私安全保護 能力	安全與隱私 保護	
		霧運算、 邊緣運算	線上訓練	資料蒐集功能	依需求調度運算資 源能力	穩定性	

圖 17、6G 之 AI-Native 3 個要素面向

資料來源：本計畫整理

6G 的 AI-Native 能提供和建構比傳統資訊與通訊科技 (Information and Communication Technology, ICT) 網路更廣闊的產業型態，整體系統可擁有更強大安全可信的「運算能量」、「AI 演算法及模型」和「資料」來源提供者，不只更加優化 6G 行動通訊系統運作效能，也架構於 AI-Native 的堅實基礎下，促使應用服務廠商能夠提供更廣、更多、更有效率、更優質的應用服務，造福行動通訊系統使用者。

四、AI-Native 技術的相關特性

AI-Native 將 AI 的技術深度融入到 6G 系統中，在上面運行的各種應用、系統和流程中的方法都可以引用 AI 功能，彰顯 AI 的普及和內化特性，基本上具有優點和一些潛在缺點，本計畫整理如下：

(一)優點

1. 自動化：AI-Native 系統可以依據實際狀況提供智慧化的決策，自動執行任務以適應情境的變化，從而提高效率和效果。

- 2.個性化：AI-Native 系統能夠根據使用者需求及偏好提供適當個性化的體驗和建議，提用戶滿意度。
- 3.即時回饋：AI-Native 系統通常能夠在偵測環境改變後，提供即時的回饋，提供用戶對應的解決方案。
- 4.優化網路管理：分析大量網路流量，可以即時優化網路資源配置、故障檢測，以提供穩定和高效的通訊服務。

(二)潛在缺點

- 1.資料隱私：AI-Native 系統需要蒐集大量的使用者資料，這引發了資料隱私，濫用或洩露資料會導致重大問題。
- 2.技術複雜性：實現 AI-Native 特徵需要複雜的技術基礎設施和各種專業知識，這對 6G 系統的開發者來說是一項挑戰。
- 3.誤用風險：AI-Native 系統可能被誤用，例如用於欺詐、虛假資訊傳播或其他不當用途。
- 4.成本：構建和維護 AI-Native 系統需要投入大量包括硬體、軟體和人員的資源和投資，成本機將大幅提高。
- 5.適應期：在實施 AI-Native 系統初期或使用者初次使用時，需要一段時間來適應和優化演算法，初期不會實現最大的效益，使用者的學習時間較久。

AI-Native 在許多方面具有潛在的優勢，其所面對但挑戰和風險，特別是在涉及到資料隱私和安全性的情況下要特別謹慎，需要較以往的系統更仔細規劃、管理和監督。

五、6G 跨領域應用及挑戰

6G 網路預期具備高傳輸、低延遲、高覆蓋與高安全特性，以支援更多設備之間的溝通，並帶來豐富且多元的資料。然而大量參與模型訓練與服務的設備，有些裝置訓練或是預測速度跟不上整體需求，或是擁有不同類別的資料而影響協同分析的正確率。為提供良好的

6G 跨領域應用服務品質與使用者體驗，需克服以下 6G 跨領域應用挑戰：

(一)大量資料與運算需求

跨領域應用中，豐富的資料將提供多元資訊來支持協同分析應用，例如物件辨識。然而，大量資料需要更多的運算效能和時間進行模型訓練，將面臨處理大量資料的挑戰，包括運算效能需求和訓練時間的壓力。

(二)短時間內模型更新

某些應用需要在短時間內快速更新辨識模型，例如智慧商店的商品辨識，由於商品變換頻繁，模型需要在短時間內完成訓練，以保持準確性和效能。

(三)新舊類別識別問題

1.新類別無法識別

在 FL 中，當面對未見過的新類別時，如圖 18 左側現有模型可能無法正確識別新類別。傳統 ML 方法通常是在訓練過程中僅針對已知的類別進行學習，而無法適應新類別，導致新類別識別率下降，影響模型的整體性能。

問題的主要原因之一是模型知識和特徵表示的不足。由於新類別的特徵分布與已知類別不同，現有的模型可能無法準確捕捉這些差異。另一個原因是缺乏足夠的標記資料來訓練新類別的辨識模型。在 FL 中，各參與者通常僅擁有部分的標記資料，這限制對新類別進行充分訓練的能力。

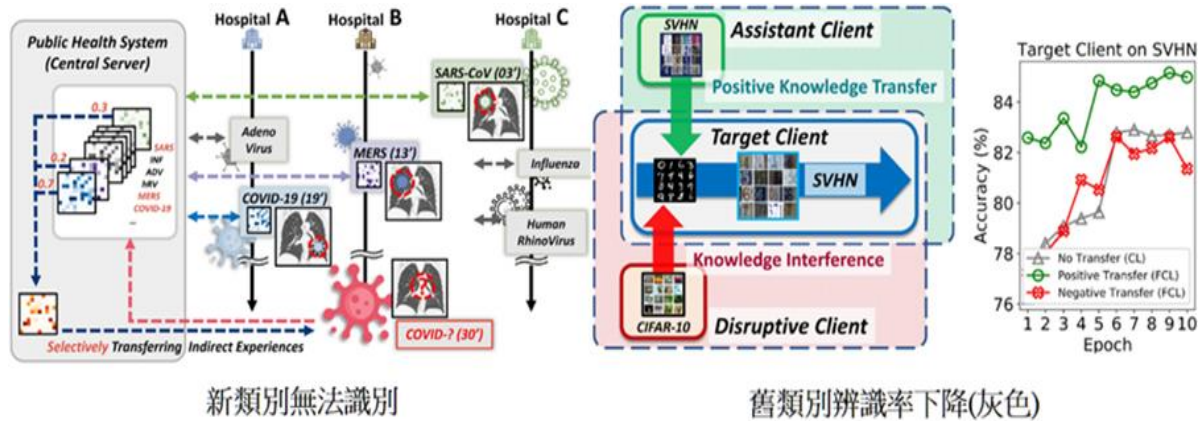


圖 18、聯合學習面臨的問題

資料來源：請參閱附錄-參考資料

這對 FL 的應用產生了重要影響。首先，當出現新類別時，模型無法對其進行準確識別，將影響相關應用的正確性和效能。其次，新類別辨識問題也對模型的擴展性產生挑戰，因為模型需要能夠適應新類別的出現，並進行快速和準確的學習。

2. 舊類別識別度下降

另外處理新類別識別問題可能會對已知的舊類別辨識率造成傷害，如圖 18 右側原模型對舊類別辨識率(灰色)會因模型開始學習新類別時，調整原有的權重和特徵表示，以適應新類別的特徵分布，可能導致對舊類別辨識率下降(紅色)，而造成的原因。

主要在於模型的適應性和遺忘性。當模型需要學習新類別時，可能會進行參數調整和特徵表示更新，以適應新類別的需求。然而，調整和更新可能會影響到原有舊類別的特徵表示，使得模型在舊類別上的辨識率下降。另一個原因是遺忘性問題，在 FL 中，當模型需要學習新類別時，可能會遺忘之前已經學習過的舊類別知識和特徵。由於模型的資源和

容量有限，當學習新類別時，模型可能需要釋放部分舊類別資源，從而導致舊類別的辨識率受損。

藉由融合 FL 與模型剪枝的技術可克服邊緣裝置計算效能不足問題，有效解決大量資料與運算需求極短時間內模型更新的挑戰，達成 6G 關鍵性能 mMTC 指標。進一步使用聯合新增類別學習(Federated Class-Incremental Learning)解決 FL 中新類別無法識別和舊類別辨識率下降 2 項重要問題，將使得 6G 通訊有更多的應用情境，例如智慧商店商品辨識和醫院疾病診斷系統。如圖 19 智慧商店商品辨識新增類別；在智慧商店商品辨識的情境下，常常需要新增類別以反映商品的變化和更新。使用 Federated Class-Incremental Learning，可以在手機端執行模型訓練，學習新商品類別，同時保持對於既有類別的辨識率，意味著當商品發生變化時，系統可以快速學習新類別，而不會影響到對於已有商品的辨識能力。

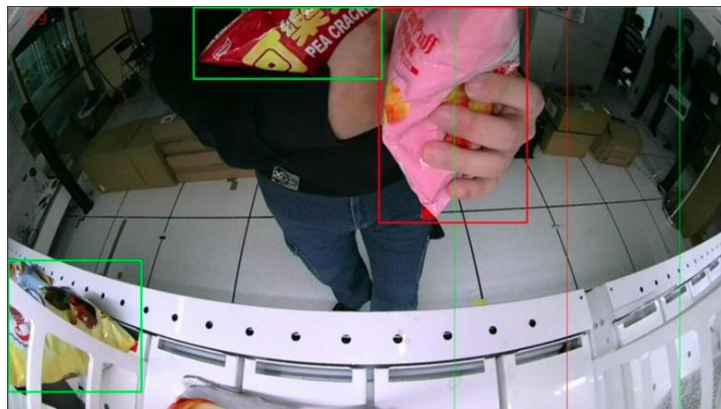


圖 19、跨領域物件辨識應用——智慧商店

資料來源：本計畫整理

另一範例為醫院疾病診斷系統的 COVID-19 學習如圖 20；在醫院疾病診斷系統中，COVID-19 疫情爆發要求系統能夠辨識和分類 COVID-19 相關影像和資料，利用 Federated Class-Incremental Learning 系統可以在手機端進行模型訓練，學習新的 COVID-19 相關類別，同

時不會對原有疾病辨識率造成影響，使得系統能夠在短時間內學習新疾病類別，同時保持對於既有疾病的準確辨識。

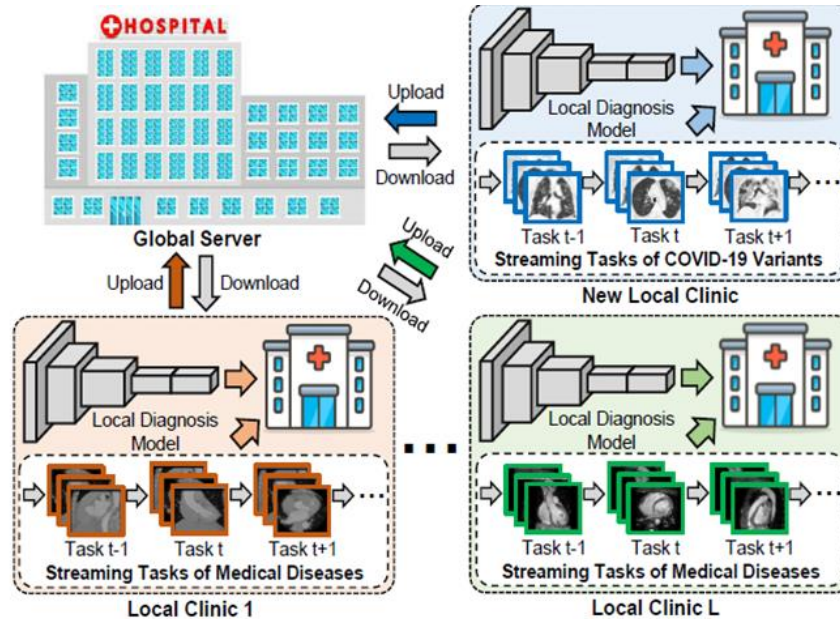


圖 20、跨領域物件辨識應用——醫院疾病診斷系統

資料來源：請參閱附錄-參考資料^{2.13}

2.13 Dong, Jiahua, et al. "No One Left Behind: Real-World Federated Class-Incremental Learning." arXiv preprint arXiv:2302.00903(2023).

第三節 跨應用層和網路層的通訊強化機制研析與方法

6G 環境預計會有大量新型的應用情境不斷涌現，不同的應用場景對通訊性能和資源需求有不同的要求，這將使得通訊需求不斷增長。本節將深入研究如何強化跨應用層和網路層的通訊機制，以及整理有助於模擬研究的適當開源軟體，用以提高 6G 網路在跨領域應用中的表現，為參考架構建立提供實質性依據。

一、跨應用層和網路層的通訊強化機制研析

跨應用層和網路層的通訊強化機制對於實現高效、可靠的通訊至關重要。跨層通訊能夠提供更全面的訊息和上下文感知，以優化網路性能和應用體驗。為實現跨應用層和網路層的通訊強化，可以考慮以下設計研究方向：

- (一)跨層訊息交換：開發新的跨應用層和網路層之間的訊息交換機制，以實現更好的協同操作和優化網路性能，包括定義跨層介面和協議，使應用層和網路層能夠有效地共享訊息和上下文。
- (二)跨層資源配置：設計跨應用層和網路層的資源配置機制，以優化資源的使用和配置，以滿足不同應用需求和網路條件，可以涉及動態配置頻寬、功率、儲存等資源，以達到最佳的性能和效能。
- (三)優化網路路由和調度：開發新的路由和調度演算法，將應用層和網路層的需求納入考慮。可以包括基於應用層需求的路由策略、跨層調度演算法，以及動態調整網路配置以滿足不同應用的要求。
- (四)跨層安全和隱私保護：強化跨應用層和網路層之間的安全和隱私保護機制，包括設計跨層的加密、身分驗證和資料隱私保護機制，以確保資料和通訊的安全性和隱私性。
- (五)協同優化和學習：開發協同優化和學習方法，使應用層和網路層能夠通過交互學習和協同優化來改進性能。可以涉及跨層的

協同學習演算法、參數優化方法等，以提高網路的效能和應用的體驗。

二、跨應用層和網路層的通訊強化方法

前述跨應用層與網路層的通訊強化機制研究方向，可藉由適當的開源軟體來模擬探索以實現更高效、靈活和智慧的 6G 通訊網路，為各個應用領域帶來更多創新和潛力，推動 6G 技術發展和應用的實現。本計畫整理目前使用最多的開源軟體如表 14，將有助於模擬進行上述研究。

表 14、開源軟體應用一覽表

	NS-3	OMNeT++	OpenAirInterface	Mininet
最新版本	ns-3.38 (2023)	OMNeT++ 6.0.1(2022)	OAI Public License V1.1. (2022)	Mininet 2.3.0 (2021)
Google scholar (since 2019)	14600 (ns-3 simulator)	1580 (OMNeT++)	1600 (OpenAirInterface)	1650 (Mininet wifi)
社群討論	Google groups: ns-3-users (約 23k 則討論)	Google groups: OMNeT++ Users (約 20k 則討論)	官網有成立群組 https://openairinterface.org/	Google groups: mininet-wifi-discuss (約 1.5k 則討論)
Annual meeting	Workshop (since 2013)	Summits (since 2008)	Workshop (Since 2016)	N/A
Sponsors	U.S. National Science Foundation	有商用版 (OMNEST)	Founding member : EURECOM Strategic Members : Qualcomm, Meta...	Mininet community

	NS-3	OMNeT++	OpenAirInterface	Mininet
其他	官網較正式 完整統計資訊 (如下載 72k 次、社群人數 8183)	N/A	N/A	Wins ACM SIGCOMM Test of Time Paper Award (使用 Mininet 進 行實作)

資料來源：本計畫整理

在探索跨應用層與網路層通訊強化機制的研究方向時，選擇適當的工具和平臺來進行驗證和模擬是至關重要的。在這個領域中，有一些知名的開源軟體工具，如 NS-3、OMNeT++、OpenAirInterface 和 Mininet，可以用來模擬 6G 通訊網路，以實現更高效、靈活和智慧的通訊系統。然而，在進行 6G 跨領域情境驗證時，需要謹慎考慮開源軟體的限制：

(一)NS-3

NS-3 可能在處理跨應用層和網路層的情境時面臨限制，因為它的主要關注點在於網路層模擬。若要涵蓋更高層次的應用通訊與交互，NS-3 可能需要進行額外的擴充和自定義，這可能增加開發和配置的複雜度。

(二)OMNeT++

OMNeT++是基於離散事件模擬的工具，在涉及大規模網路和複雜的通訊協定情境時，可能面臨模擬效能方面的挑戰。因此，對於 6G 中可能存在的高密度、高互聯性的網路環境，OMNeT++可能需要優化和調整，以確保準確的模擬結果。

(三)OpenAirInterface

OpenAirInterface 是一個針對無線通訊網路的開源軟體，適用於研究蜂窩和無線接入技術。6G 跨領域的應用情境可能超出 OpenAirInterface 的主要設計目標範圍。

(四)Mininet

Mininet 是一個用於 SDN 環境的模擬器，主要用於研究網路架構和協定。然而，若要深入探索跨應用層與網路層的通訊強化機制，Mininet 可能需要進一步的擴充和修改，以支援更高層次的應用和通訊場景。

因此在進行跨領域情境驗證時，可能需要考慮使用其他更全面、更真實的方法和平臺，以確保研究結果更加可靠，更貼近實際 6G 通訊網路的特點，整理如下：

(一)模型準確性和複雜度限制

模擬 6G 通訊網路時，需要考慮到更多的複雜性和多樣性。可能涉及到更高精度的模型，以捕捉不同應用和網路場景的特定要求。

(二)跨層級整合

6G 通訊網路涉及多個層級的交互作用，從物理層到應用層，需要進行全面的跨層級驗證。某些開源工具可能主要專注於特定層級，無法提供足夠的支援來模擬多層級互動和優化。

(三)協議和技術支援

6G 預計將引入許多新的通訊協議和技術，這可能無法得到部分開源軟體的即時支援或正確實現。

(四)實驗平臺限制

一些 6G 研究可能需要更接近真實網路環境的實驗平臺(如手機)，以進行實際測試和驗證。手機系統通常需要高度的定制性和優化，以確保 6G 跨領域應用的高效運行。然而，開源軟體可能有以下限制，無法提供足夠的彈性，以滿足這些需求。



1. 不足的定制性：開源軟體難以定制以適應特定的 6G 跨領域應用，特別是在基於手機系統(如 Android)的情境下。手機應用的需求多樣化，需要能夠充分適應各種不同場景。
2. 限制的彈性：開源軟體可能不具備足夠的彈性，以適應 6G 跨領域應用的複雜性，尤其是在基於 Android 手機系統的環境中。這些應用需要高度可定制和可擴展的解決方案。
3. 效能挑戰：跨領域的 6G 應用通常對於低延遲和高頻寬有著高要求。開源軟體可能無法提供足夠的效能以滿足這些需求，尤其在資源受限的 Android 手機系統上。

第四節 跨領域應用情境實證與雛型系統先導評估

一、實證目的

為因應 6G 跨領域應用挑戰，使用 Federated Class-Incremental Learning 進行物件辨識應用驗證是一個有價值的研究方向；藉由 Federated Class-Incremental Learning 技術，可以在跨設備和分散式環境下進行模型訓練和更新，在新增類別的同時也不會影響既有類別的辨識率，這種方法特別適合手機端執行物件辨識應用。傳統機器學習會是在封閉環境中使用固定的資料集進行訓練，資料集是要預先準備好的，然而在現實世界的應用中，資料會是以數據流方式源源不斷地產生，在運算資源和效率的考量下，這個情況會影響到模型的適應性，並且會出現名為災難性遺忘 (Catastrophic Forgetting) 的現象發生，在不斷學習新任務的情況下，模型會忘記原本學到的知識，因此為了能讓模型在接收新數據時，能持續學習和改進，會需要使用到增量學習 (Incremental Learning) 來訓練模型。

本計畫預計將會進行智慧商店商品辨識新增類別的跨領域應用情境實證，以及使用 CIL 進行實作並與傳統機器學習演算法比較正確率，本實證計畫能夠達成目標如下：

- (一) 在跨設備和分散式環境下，進行模型訓練和更新。
- (二) 在新增類別的同時，不會影響到既有類別的辨識率。
- (三) 模型能夠持續辨識新類別。

二、測試方法

本計畫參考類別增量協作學習 (Co-Transport for Class-Incremental Learning, COIL) 論文^{2.14}，開發智慧商店商品辨識新增類別系統 (System of Class-Incremental Learning, SCIL)，以下將介紹 COIL 演算法及 SCIL 系統。

2.14 Da-Wei Zhou, Han-Jia Ye, De-Chuan Zhan (2021) Co-Transport for Class-Incremental Learning. Retrieved from <https://arxiv.org/pdf/2107.12654.pdf>

(一)COIL 演算法

新類別和舊類別之間存在著一些相聯關係 (Semantic Relationship)，COIL 會將新舊類別映射在一個空間，以此度量類別間的關係，距離越近代表關聯性越大，並使用最佳傳輸 (Optimal Transport) 來最小化模型更新所需的代價，如圖 21 及圖 22 所示。最佳運輸分為 2 個方面，向前傳輸 (Prospective Transport) 利用最佳傳輸所獲得之新舊知識整合分類器來做為訓練新分類器的初始化，與原始使用隨機生成相比，能夠提升模型學習的效率；向後傳輸 (Retrospective Transport) 則將新分類器轉換為舊分類器，以防止災難性遺忘。因此，模型所學得知識可以在增量學習的過程中雙向流動，進而在學習新類別的同時，也能保留對舊類別的認知。

以下為 COIL 演算法說明：

1. 學習新類別的任務到來時，假設當前是第 b 次任務，開始做向前運輸，呼叫 OT 函數來快速初始化新分類器 W_{new} ，OT 的輸入參數分別有舊資料 $\mathcal{E}_{b-1}$ 、新資料 D^b 和舊分類器 W_{old} ， W_{new} 是在參考新舊類別之間的關係後，由 W_{old} 做矩陣轉換而輸出的分類器
2. 做總訓練資料的更新
3. 進入迴圈 (定義 epoch 數)
4. 導入這一輪訓練資料
5. 計算向前 Loss L_{PT}
6. 做向後運輸，呼叫 OT 函數來輸出 $\hat{W}_{\text{old}}$ ，將新分類器 W_{new} 轉換為舊分類器 $\hat{W}_{\text{old}}$ ，每一次迴圈都會做一次，以此避免災難性遺忘的發生
7. 計算向後 Loss L_{RT}
8. 計算整體 Loss L_{COIL}
9. 更新模型

10.重複迴圈直到完成定義之 epoch 數

Algorithm 1 Co-transport for incremental learning

Input: New task instances: $\mathcal{D}^b$; former exemplars: $\mathcal{E}_{b-1}$;

Output: Updated model

```

1:  $W_{new} = OT(\mathcal{E}_{b-1}, \mathcal{D}^b, W_{old});$  ▷ Fast initialization
2:  $\mathcal{D}_{train} = \mathcal{D}^b \cup \mathcal{E}_{b-1};$  ▷ Rehearsal
3: repeat
4:   Get a batch of instances;
5:    $\mathcal{L}_{PT} \leftarrow \text{Eq. 4};$  ▷ Prospective transport loss
6:    $\hat{W}_{old} = OT(\mathcal{D}^b, \mathcal{E}_{b-1}, W_{new});$ 
7:    $\mathcal{L}_{RT} \leftarrow \text{Eq. 5};$  ▷ Retrospective transport loss
8:    $\mathcal{L}_{COIL} \leftarrow \text{Eq. 9};$  ▷ Total loss
9:   SGD over  $W_b$  and  $\phi(\cdot);$  ▷ Update model
10: until reaches predefined epochs

```

圖 21、COIL 演算法

資料來源：請參閱附錄-參考資料^{2.14}

上述 COIL 演算法會在第 1 步模型訓練前呼叫一次 OT 函數，並在第 6 步模型訓練後再呼叫一次 OT 函數，2 次 OT 函數是共用的，也因此每個任務新增的類別數量為固定值。而本實證計畫調整了演算法，對第 1 步 OT 函數進行修正，使得函數可以根據新任務的類別數量進行調整，產生新的 W_{new} 。

以下為最佳傳輸演算法說明：

- 1.輸入參數有原始資料、目標資料和原始分類器
- 2.計算每個類別的映射中心
- 3.由類別的映射中心計算 2 類別的距離 $C_{n,m}$ ，距離越大，則代表 2 個類別的相似度越小
- 4.最佳化計算，目標是產生能夠滿足最小化總距離成本 C 的轉移矩陣 T

2.14 Da-Wei Zhou, Han-Jia Ye, De-Chuan Zhan (2021) Co-Transport for Class-Incremental Learning. Retrieved from <https://arxiv.org/pdf/2107.12654.pdf>

- 5.讓 T 和 W_o 做矩陣相乘，產生目標分類器 W_g ，代表 W_g 在參考原始資料和目標資料後，由 W_o 轉換而來的，具有辨識新舊知識的能力

Algorithm 2 OT for classifier transportation

Input: Origin exemplars: $\mathcal{E}_o$;

Goal exemplars: $\mathcal{E}_g$;

Origin classifier: W_o ;

Output: Transported goal classifier W_g ;

- 1: **function** OT($\mathcal{E}_o, \mathcal{E}_g, W_o$)
 - 2: Class center of embeddings $\leftarrow$ Eq. 7;
 - 3: Transportation cost $C \leftarrow$ Eq. 8;
 - 4: Solve OT problem in Eq.6; get transport mapping T ;
 - 5: **return** $W_g = TW_o$
-

圖 22、最佳傳輸演算法

資料來源：請參閱附錄-參考資料^{2.14}

(二)SCIL 系統

為更貼切符合 6G 跨領域實際場域應用，本計畫開發 APP 模擬真實世界使用者情境，共有 3 個功能，分別說明如下：

- 1.模型應用：可上傳圖片並顯示預測結果，使用流程如圖 23：

- (1)點選模型應用，切換至模型應用介面
- (2)點擊 upload 按鈕選擇要預測的圖片
- (3)接著會將圖片上傳至伺服器，模型辨識類別後回傳結果至應用程式，並顯示辨識結果

2.14 Da-Wei Zhou, Han-Jia Ye, De-Chuan Zhan (2021) Co-Transport for Class-Incremental Learning. Retrieved from <https://arxiv.org/pdf/2107.12654.pdf>



圖 23、模型應用示意圖

資料來源：本計畫整理

2.新資料上傳：上傳新類別圖片進行模型訓練，使用流程如圖

24：

- (1)點選新資料上傳，切換至上傳資料介面
- (2)輸入 gid、Name、Weight、Tag 等資訊(gid 需由純數字組成)
- (3)點擊 Load，選擇多張照片
- (4)點擊 Upload，上傳選擇的多張照片至 Server，並根據 gid 儲存在 Server 的資料夾內
- (5)點選 Start，使用上傳的資料訓練模型
- (6)由伺服器回傳狀態，有「模型開始訓練」、「已有模型訓練中，尚須 X 分鐘完成」及「無新資料，無須訓練」3 種可能性



圖 24、上傳資料示意圖

資料來源：本計畫整理

3.產品內容：如圖 25 按下「產品內容」鈕後顯示目前可辨識的商品類別。



gid	goods_name
31369	(A)*純喫茶紅茶650ml(盒)
36225	*瑞穗蘋果牛奶290ml
119601	統一麵肉燥風味(碗)
119753	(A)滿漢大卷筒燒牛肉麵
130556	統一布丁--雞蛋口味
131337	*藍山咖啡CAN240
158660	*統一麥香奶茶TP375
173920	統一脆麵
181992	阿Q桶麵主粒海鮮風味
185967	樂天小熊餅(巧克力)
286813	(A)*可口可樂PET600
292595	茗聞情凍頂烏龍茶
307561	(A)科學麵原味
320220	品客洋芋片-洋蔥(小)
346960	來一客杯麵韓式泡菜風味
353494	美麗日記黑珍珠煥白8入
354850	美麗日記官燕窩全效滋養8入
358392	靠得住草本抑菌夜用28cm12片
361375	iselect麥茶PET550ml
367494	蘇菲超熟睡超薄棉柔28cm15片

圖 25、產品內容統整示意圖

資料來源：本計畫整理

三、測試環境及架構

測試系統環境設定，如硬體、作業系統選擇等具備以下要件：

- (一)硬體設備選擇：適合的設備可以確保系統在運行時有足夠運算能力和 RAM，例如智慧手機或嵌入式裝置。
- (二)作業系統和開發環境：根據所選硬體設備，選擇適合的作業系統，例如 Android 或 iOS。安裝相應的開發環境，例如 Android Studio 或 Xcode，以進行程式開發和編譯。
- (三)模型訓練和部署工具：選擇適合的 ML 框架和工具，以訓練和部署辨識模型，常見選擇包括 TensorFlow、PyTorch、Keras 等，確保在所選環境中安裝並配置相應的工具。
- (四)資料收集和標註：確定用於訓練和驗證的資料集，可以使用現有公共資料集，或通過自行收集並進行標註。
- (五)模型訓練：使用所選的 ML 框架，設計和訓練辨識模型。使用已有的類別資料進行初始訓練，並在需要新增類別時，使用包含新類別的資料進行增量訓練。
- (六)模型部署：在選擇的硬體設備上部署訓練好的模型，可能涉及將模型導入應用程式代碼中，進行適當的模型載入和初始化。
- (七)模型更新機制：設計一個機制來處理新增類別的模型更新，包括檢測並下載新的模型權重或模型結構，在應用程式中進行模型切換和更新。
- (八)性能優化：進行必要的性能優化措施，以確保模型在手機端運行時的效能和效率，包括模型壓縮、量化和硬體加速等技術。

本計畫用戶端(Client)以手機做為介面，可以拍照上傳資料至伺服器(Server)進行新類別訓練或接收辨識結果，並顯示於螢幕等 2 種功能；Server 則接收不同用戶上傳的資料，根據需求進行模型訓練或回傳辨識結果，詳如圖 26 所示。

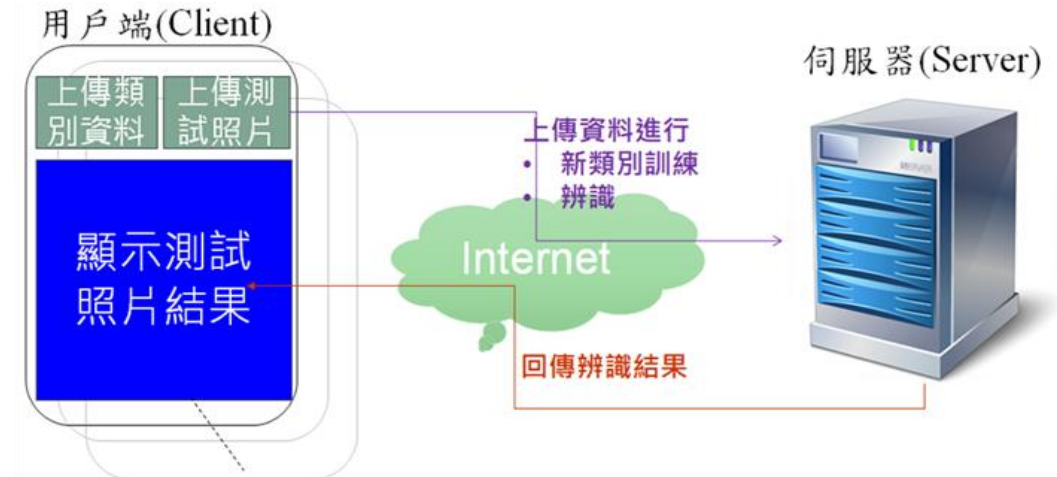


圖 26、跨領域應用情境實證與雛型系統-應用情境架構示意圖

資料來源：本計畫整理

四、使用之軟硬體

本實證應用情境之 Sever 及 Client 使用軟硬體規格，詳如表 15 及表 16 所示。

表 15、Server 軟硬體規格

名稱	Server	
硬體規格	- Intel (R) Core (TM) i9-10980XE CPU @ 3.00GHz 18cores 64GB RAM 512 GB HDD - NVIDIA GeForce RTX 4090	
作業系統	Ubuntu 22.04.1	
程式軟體	- Driver Version: 535.86.05 - CUDA Version: 12.2 - conda 23.7.2 - python 3.7.16 - torch 1.13.1 - torchaudio 0.13.1 - torchvision 0.14.1 - POT 0.9.0 - Flask 2.1.1 - Pandas 1.3.5	
網路介面	cat6	
備註	此伺服器為透過 VMware vCenter Server 8.0.0 伺服器管理軟體所架設之虛擬機	

資料來源：本計畫整理

表 16、Client 軟硬體規格

名稱	Client
硬體規格	• Xperia 5 II • Qualcomm Snapdragon 865, 2.8GHz + 1.8GHz 八核心處理器 • 8GB RAM • 256GB UFS
作業系統	Android 12
程式軟體	工研院_跨領域應用情境實證應用程式
網路介面	IEEE802.11a/b/g/n(2.4GHz)/n(5GHz)/ac/ax
備註	「工研院_跨領域應用情境實證應用程式」為自行開發之 Andriod App，透過 APK 檔進行安裝

資料來源：本計畫整理

五、測試步驟

在 SCIL 系統架構下，實證將比較 CIL 演算法及卷積神經網路 (Convolutional Neural Networks, CNN) 演算法的正確率；CNN 是一種 DL 模型，可藉由卷積操作自動地從影像中提取特徵，使其在處理影像相關的任務非常成功。因此 CNN 成為研究人員和工程師首選的工具，並且成為許多深度學習領域的基準模型。大部分 ML 和 DL 競賽、研究和應用中都會選擇 CNN 來進行比較，原因如下：

(一)CNN 在影像相關任務中表現卓越：如像物件識別、物件檢測及物件分割等。

(二)預訓練的模型可用性：有許多預先訓練好的 CNN 模型（如 VGG、ResNet、Inception、MobileNet 等），這些模型在大型影像資料集上進行訓練，並在各種應用中提供了出色的基礎性能。研究人員和工程師可以使用這些預訓練模型，並對其進行微調以適應特定任務。

- (三)參數共享和平移不變性：CNN 的卷積層使用參數共享，這使得它能夠捕捉物體的平移不變性，即不論物體在影像中的位置如何，CNN 仍能夠識別它。這種特性對影像辨識非常重要。
- (四)網路的深度和複雜性：CNN 通常是深度網路，具有多個卷積層和全連接層，這使它能夠學習多層次的抽象特徵。
- (五)豐富的研究支持：CNN 經過多年的研究和發展，有許多開源框架（如 TensorFlow、PyTorch、Keras 等）支援 CNN 的實作，使得研究人員和工程師能夠輕鬆地應用和擴展這些模型。
- (六)多領域應用：CNN 不僅在影像處理中成功，還在語音識別、自然語言處理、遊戲和其他領域取得了優異成就，因此 CNN 被廣泛應用於各種不同的應用中。

本實證計畫測試步驟如圖 27 所示：

- (一)Server 預訓練一影像分類模型(Resnet 18 架構作為 Backbone)
- (二)Client 上傳新類別訓練資料至 Server
- (三)Server 接收 Client 上傳資料，只以當下資料更新既有的 CNN 及 CIL 模型
- (四)Client 上傳測試影像(舊+新類別)至 Server
- (五)Server 接收各項 Client 上傳測試影像，並分別回傳 CNN 及 CIL 模型辨識結果
- (六)Client 接收辨識結果並顯示在手機螢幕計算正確率
- (七)回步驟 2

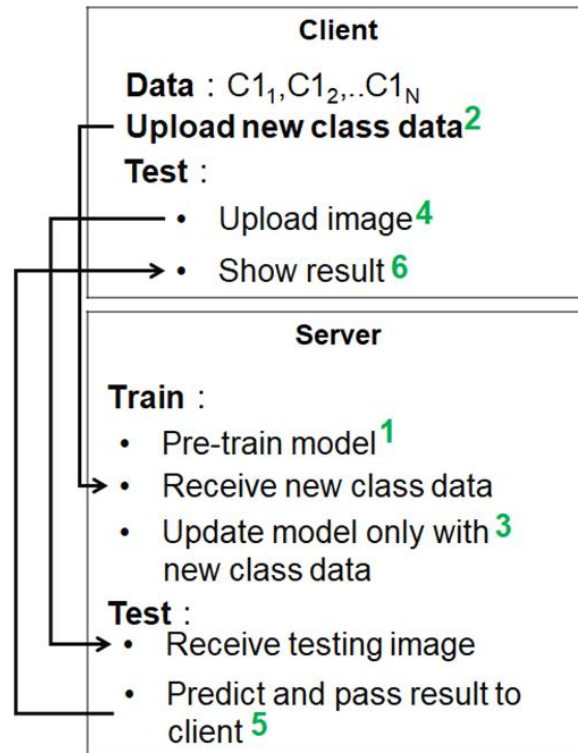


圖 27、跨領域應用情境實證與雛型系統-測試步驟示意圖

資料來源：本計畫整理

六、測試數據及測試結果之探討

(一)CIL 改善 COIL 實證問題

SCIL 系統中，COIL 演算法僅能在第 1 次新增類別時設定數量，而隨後新增的類別數量必須維持不變，例如第 1 次新增 10 類，之後每次新增就只能是 10 類，這顯然不符 6G 實際應用時的需求，無法要求每個參與的使用者上傳相同數量的類別。本計畫對此策略進行修改，使得類別數的設定更具靈活性；除了保持沒有限制第 1 次新增類別的數量外，之後每次也可以任意選擇增加的類別數，以符合實際應用需求。

另外，COIL 原先使用的超參數設定如下：

1.迭代次數(Epoch)：160

2.批次大小(Batch_size)：128

3.訓練/測試資料比例：80% for training、20% for testing

4. 優化器 (Optimizer)：SGD

5. 學習率 (Learning rate)：0.1

其中學習率為控制模型中梯度下降的速度，公式為：新權重 = 舊權重 - 學習率 * 梯度。Learning rate 的設置很重要，如下圖 28，設置過小時，會導致模型學習收斂較慢，且容易過擬合 (Overfitting)。而設置過大時，會容易導致模型學習過快，無法收斂。使用梯度下降進行優化，幾乎是所有優化器的核心概念，而其中 2 個重要的項目：

1. 決定前進的方向是否正確 (優化方向)，在優化器中反映為梯度或動量。
2. 決定每一步要走多遠 (步長)，在優化器中反映為學習率。

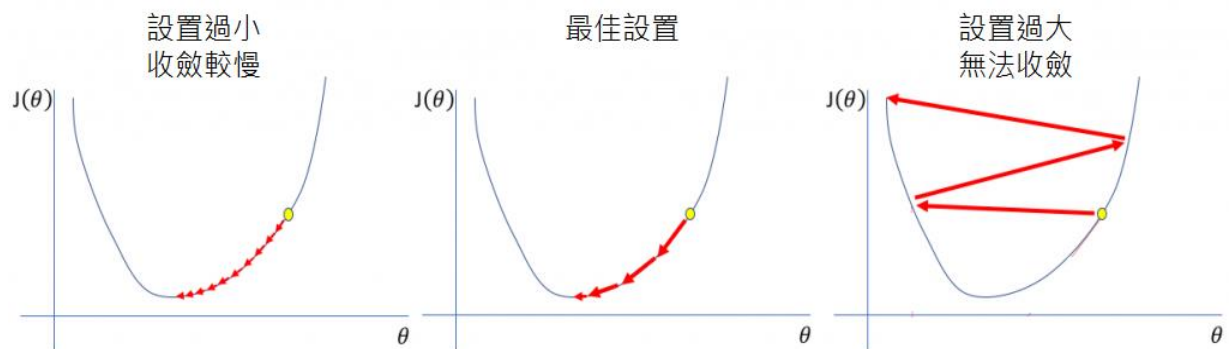


圖 28、商品資料集學習率

資料來源：請參閱附錄-參考資料^{2.15}

以下介紹 3 種常見的優化器：

1. 隨機梯度下降法 (Stochastic Gradient Descent, SGD)

透過計算每個訓練樣本的梯度來更新模型參數。它是一種基礎的優化演算法，透過對每個樣本進行梯度計算，逐步調整模型參數。SGD 缺點是在雜訊較大或參數更新不穩定時可能導致訓練過程震盪或收斂速度慢。

2.15 Medium. (2020) Retrieved from <https://gino6178.medium.com/%E6%A8%A1%E5%9E%8B%E5%A3%93%E7%B8%AE%E5%8F%8A%E5%84%AA%E5%8C%96-learning-rate-c340a0b940e4>

2.Adam：A Method for Stochastic Optimization

一種結合動量 (Momentum) 和自適應學習率 (Adaptive Learning rate) 的優化算法。通常能夠在訓練過程中更有效地調整學習率，並在不同參數有不同尺度的情況下適應性地更新參數，有效改善 SGD 的缺點，但有可能無法收斂而降低模型泛化能力 (Generalization)。

3.AdamW

Adam 優化算法的一種變種，引入權重衰減 (Weight decay) 的概念，將權重衰減與優化算法的步驟分開處理，更準確地對模型的權重進行衰減。AdamW 通常能夠提高模型的泛化能力，特別是在避免過擬合方面效果顯著。

在此設定下，光訓練一個類別就超過 13 小時，這明顯也不符合 6G 實際應用時的需求，例如智慧商店要販賣若干新品項，須得等上幾天才能上架，可能就會發生檔期延誤的問題。因此為了節省訓練時間，本計畫對各項超參數進行調整與測試；首先將批次大小設定為 512，並且使用 AdamW 作為優化器，使模型的收斂速度更快，減少整體訓練時間。接著考量到每一類的訓練時間不宜太長，因此針對訓練資料比例、迭代次數及學習率這 3 個參數進行調整，並進行正確率測試。當訓練資料比例為 80% 及 50% 時，雖然可以得到較優秀的正確率，但所需要花費的時間較長；而若只有 15% 得到的正確率則又過低，因此最終選擇 30% 作為訓練資料比例 (實際照片張數約為 600 張)，詳如表 17。在這個比例下，嘗試多種不同的迭代次數 (分別為 60、30、20) 和學習率 (0.1、0.3、0.4) 的組合，以平衡高正確率和合理的訓練時間。最終選擇迭代次數為 30 和學習率為 0.3 的組合，這樣可以在保持訓練效果的情況下，不增加太多訓練時間。

以下整理本計畫實驗(包含 CIL 及 CNN)使用的超參數^{2.16}：

- 1.迭代次數(Epoch)：30
- 2.批次大小(Batch_size)：512
- 3.訓練/測試資料比例： 30% for training、70% for testing
- 4.優化器(Optimizer)：adamW
- 5.學習率(Learning rate)：0.3

表 17、參數調整對應準確率及時間

訓練資料 比例	迭代次數	學習率	單一類別 最低測試 正確率	平均測試 正確率	增加一類所 需時間 (min)
80%	60	0.1	94.46%	98.85%	300
50%	60	0.1	93.17%	98.38%	210
50%	30	0.1	82.68%	95.67%	98
30%	30	0.1	55.88%	91.96%	61
30%	30	0.3	71.26%	94.32%	63
15%	30	0.4	61.55%	85.67%	62
30%	20	0.3	39.17%	74.22%	46
30%	20	0.4	8.99%	76.39%	47

資料來源：本計畫整理

6G 網路的一個特點是提供更高的頻寬，這對於傳輸大型 CNN 和 CIL 模型至關重要。高頻寬才能負荷在短時間內傳輸大量的模型參數，如上千種品項的智慧商店。另外，6G 網路的低延遲特性對於在邊緣端(Edge)進行即時決策的應用非常重要，模型在每個回合內消耗的時間和資源都必須是高效的，以便快速響應需求。例如，在智慧工廠中，ML 模型需要在較短的時間內執行，以監控和優化

2.16 GitHub. yfjeffliu/itri_cil_goods. Retrieved from https://github.com/yfjeffliu/itri_cil_goods

生產流程；或是在智慧城市中，監控系統可以利用 6G 網路傳輸數據到邊緣伺服器，進行即時影像分析以檢測交通違規和犯罪活動。

(二)實驗設計及應用程式說明

本計畫共收集 50 類商品，每類商品約 2,000 張影像如圖 29 所示，以 80%及 20%的比例分為訓練及測試資料集。首先各分 25 類商品給 Client 1 及 Client 2，模擬不同使用者擁有不同的資料，接著以協同學習概念逐次將資料上傳，使得使用者本身及其他使用者都可以學到新知識，而 Server 有其硬體限制如 RAM、運算效能等，無法將所有資料皆拿來訓練並產生一個難以想像的龐大模型，因此 Server 只能以每次上傳的新資料來訓練模型，如此也才能符合真實世界的設定。本計畫藉由以下任務(Task)逐次增加商品類別，並根據上述實驗步驟來比較 CIL 演算法及 CNN 演算法的正確率：

- 1.Task0：Client 1 上傳 20 類商品訓練，測試 C1~C20 類商品正確率。
- 2.Task1：Client 2 上傳 20 類商品訓練，測試 C1~C40 類商品正確率。
- 3.Task2-Task11：Client 1、2 分別逐次上傳 1 類商品，測試 C1~C41 - C1~C50 類商品正確率。

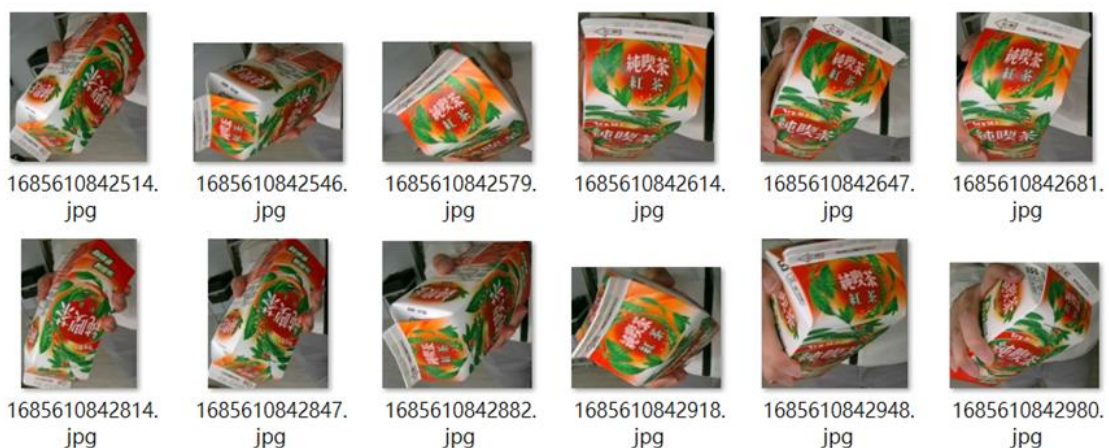


圖 29、商品資料集

資料來源：本計畫整理

(三)實驗結果

本實證計畫所使用之 CIL 演算法及 CNN 演算法的正確率比較，結果顯示 CIL 演算法明顯優於 CNN 演算法，不會因類別增加而影響辨識正確率，如圖 30 所示。

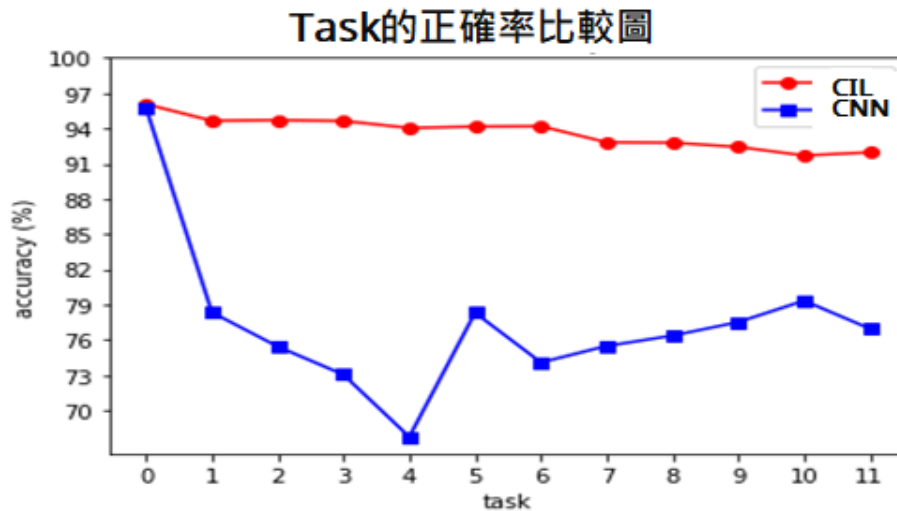


圖 30、Task 正確率比較圖

資料來源：本計畫整理

另外以長條圖詳細分析準確率的分佈，其中橫軸為準確率的區間，縱軸為該準確率區間的類別數量，如圖 31 所示。左圖為 CIL 演算法，右圖為 CNN 演算法，可以發現 CIL 演算法有超過 8 成類別之辨識正確率達 90%以上，成效明顯優於 CNN 演算法。

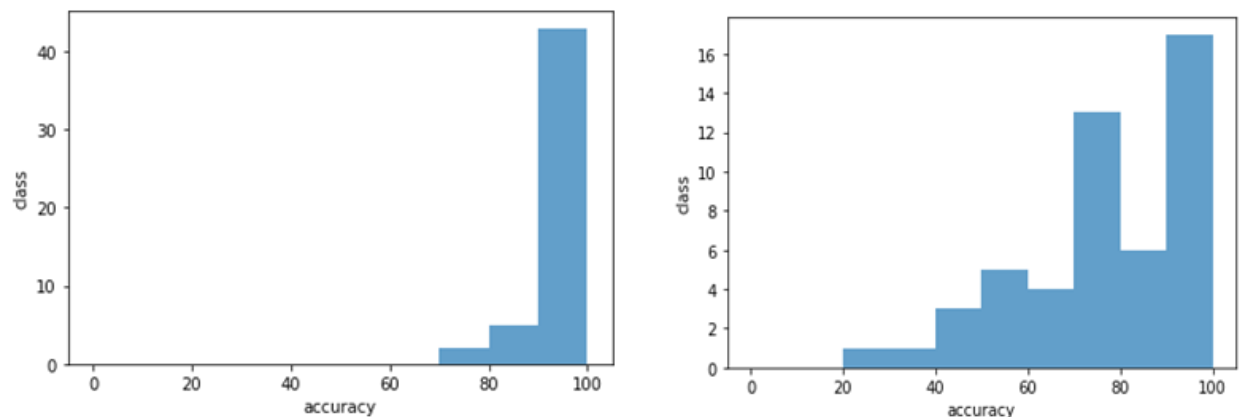


圖 31、準確率區間比較圖

資料來源：本計畫整理

(四)實驗結果分析

1.運算時間比較

CNN 及 CIL 模型大小接近，以完成 11 項任務可分 50 類的模型為例，參數量分別為 11202162 及 11714601，模型預測時間同為 0.06 秒(包含模型與圖片讀取)，在沒有進行任何模型優化(如模型剪枝)的情況下，應都符合 6G 跨領域應用的即時性要求。表 18 整理了每項任務中 CNN 及 CIL 對於新/舊類別的測試正確率，以及所需的訓練時間。CIL 在每項任務中，新/舊類別的正確率差異小(<3%)；CNN 則是新/舊類別的正確率差異極大，但對於新類別會有較好的辨識正確率以及所需的訓練時間較少(約為 CIL 的 6 成)。這意謂在某些不需新增類別的應用，CNN 也許會是較好的選擇。例如固定類別的物件辨識(如野外使用應用程式辨識植物)，在 6G 網路下可以快速收集不同使用者的多元資料，可專注精進既有類別的辨識正確率，效能會比 CIL 佳。

表 18、CNN 與 CIL 演算法舊/新類別準確率與時間比較

Task	訓練資料類別	測試資料類別 舊類別 新類別	CNN 演算法 舊類別正確率 新類別正確率 花費時間(min)	CIL 演算法 舊類別正確率 新類別正確率 花費時間(min)
0	C1~C20	C1~C20 N/A	95.73% N/A 23 min	95.86% N/A 19 min
1	C21~C40	C1~C20 C21~C40	57.88% 98.82% 30 min	94.77% 98.47% 142 min
2	C41	C1~C40 C41	74.81% 99.70% 36 min	96.30% 98.00% 61 min

Task	訓練資料 類別	測試資料類別 舊類別 新類別	CNN 演算法 舊類別正確率 新類別正確率 花費時間(min)	CIL 演算法 舊類別正確率 新類別正確率 花費時間(min)
3	C42	C1~C41 C42	72.48% 99.43% 36 min	96.14% 98.71% 61 min
4	C43	C1~C42 C43	67.04% 99.80% 37 min	95.80% 95.36% 61 min
5	C44	C1~C43 C44	77.83% 99.87% 38 min	95.79% 98.08% 61 min
6	C45	C1~C44 C45	73.45% 99.77% 39 min	95.69% 97.23% 63 min
7	C46	C1~C45 C46	74.86% 99.89% 39 min	95.17% 96.18% 64 min
8	C47	C1~C46 C47	75.92% 99.09% 40 min	95.01% 97.97% 65 min
9	C48	C1~C47 C48	77.04% 99.31% 42 min	94.59% 94.83% 65 min
10	C49	C1~C48 C49	78.89% 98.96% 42 min	94.20% 96.96% 67 min
11	C50	C1~C49 C50	76.52 99.39 42 min	94.30 95.55 66 min

資料來源：本計畫整理

2.錯誤案例分析

分別舉例說明 CNN 及 CIL 預測錯誤的範例：

(1)部分商品類別 2 個模型都沒有辦法取得較高正確率，通常是因為擷取的圖片沒有該類別明顯的特徵，如泡麵底部、飲料瓶身(無包裝的部份)或是圖片過於模糊等，如表 19，這些因取得影像品質不佳造成的錯誤，應由其他方法解決。

表 19、CNN 與 CIL 正確率皆較低之案例(CNN<90% CIL<90%)

測試圖片	圖片類別	CNN 預測類別	CIL 預測類別	錯誤類別範例圖片
	滿漢大餐 蔥燒牛肉 麵	來一客杯 麵韓式泡 菜風味	阜杭豆漿- 經典飯糰	
	維力炸醬 麵重量碗	韓國農心 辛香菇杯 麵	韓國農心 辛香菇杯 麵	

資料來源：本計畫整理

(2)商品類別若與最後一個 Task 新增之類別有較高的相似性，CNN 就容易判斷成最後一個 Task 的商品類別，但 CIL 無此問題。這也證明 CNN 偏重學習新類別的特徵，易遭受災難式的遺忘而無法辨識舊類別，如表 20。

表 20、CNN 正確率較低 CIL 正確率正常案例(CNN<90% CIL>90%)

測試圖片	圖片類別	CNN 預測 類別	CIL 預測 類別	錯誤類別範例圖片
	統一布丁- 雞蛋口味	(區)日式 素豆干立	統一布丁-- 雞蛋口味	
	阿華田營 養巧克力 麥芽飲品	(區)日式 素豆干立	阿華田營 養巧克力 麥芽飲品	

資料來源：本計畫整理

(3)在圖片清晰的狀況下 CNN 與 CIL 通常都能夠正確預測商品類別，然而 CIL 在部分的類別極為相似時無法分辨，相對地 CNN 則有較好的表現。原因應是 CIL 為兼顧新/舊類別的辨識正確率，提取的特徵只要足以分辨彼此即可，而 CNN 則會專注提取較精細的特徵以取得對新類別更高的辨識正確率，如表 21。

表 21、CNN 正確率正常 CIL 正確率較低案例(CNN>90% CIL<90%)

測試圖片	圖片類別	CNN 預測 類別	CIL 預測 類別	錯誤類別範例圖片
	卡迪那德州 薯條茄汁口 味	卡迪那德州 薯條茄汁口 味	濃韻烏龍茶 PET600	
	韓國農心辛 香菇杯麵	韓國農心辛 香菇杯麵	濃韻烏龍茶 PET60	

資料來源：本計畫整理

第五節 小結

在這個日益多元和高度互聯的數位時代，6G 通訊技術將是未來網路發展的關鍵驅動力，其應用將推動社會、產業和科技向前跨越巨大的發展障礙。

首先說明建立 6G 跨領域應用情境的必要性和重要性，包括對 6G 網路特點與優勢的闡述，並著重強調 6G 技術在不同應用領域的潛在價值。接著探討 6G 應用趨勢、發展情境以及願景與 IMT-2030 發展架構，6G 應用發展趨勢多樣，必須兼容包容性(Inclusivity)、普及性、永續性、創新性(Innovation)、安全性、堅韌性(Resilience)、互助性(Interoperability)及互通性(Interworking)等多個面向，除可結合 H2H、H2M、M2M 之先進應用外，範圍更可擴及城市、工廠、交通、醫療、感測、媒體與環境等。雖然各式新興應用依據其適用環境與對象，皆有獨特發展特性與服務需求，然而，依據其使用情境，仍可歸納分析出數個特定技術需求之應用情境。6G 系統發展除了繼續延伸改進 5G 行動通訊之 3 大應用情境，即 eMBB、uRLLC 與 mMTC 之外，也將朝向「普及連線」、「AI 整合通訊」和「感測通訊整合」等 3 個新增應用情境發展，逐步朝向永續性、連所未連(Connecting The Unconnected)、安全隱私和堅韌性，以及智慧普及等 4 大總體(Overarching)目標前進。

一、Cloud-Native 應用，進行中的虛擬化趨勢

一般針對 Cloud-Native 認知即一種在雲端運算環境中建置、部署和管理應用程式的軟體方法。企業、組織可藉以建置有彈性、可擴充和靈活的應用服務，提供快速更新應用服務內容，滿足客戶需求。工程師可以進行小量、頻繁地、可預測地做出系統變更。

Cloud-Native 最顯見的技術特徵為微服務及容器，除提供在網路應用層面的實作外，網路管理層面也是提供 SDN 一種實作選擇，如容器化網路功能、微服務化的網路控制器、自動化網路配置等可以更

彈性、迅速、自動化網路效能管理機制，亦即未來 6G 無線網路環境下，Cloud-Native 技術的使用會自應用層面穿透至網路層面，將是必需重視的發展趨勢。

二、AI-Native 架構，實現自治和自動化的 6G 網路

AI 科技在理論基礎、演算法、處理手段甚至計算環境等都有突飛猛進的進展，目前業界認為 AI-Native 是未來 6G 行動網路系統的重要特徵之一，更緊密深入融合到 6G 系統架構、網路元件和作業流程之中。AI 會深度整合到 6G 網路和應用中，以實現更智慧、自主和高效的通訊環境。且基於電信基礎設施普及之優勢，智慧優化網路管理、自動化自主網路等網路效能優化特徵，將會更加彰顯出 AI-Native 在網路效能提升及所可以創造的價值，協助實現未來 6G 無線網路的願景。

基本上 6G 行動通訊系統下 AI-Native 的實現，可自能力、服務、架構技術 3 個面向觀察，考量各面向中有關運算資源、AI 演算法和資料 3 要素的需求，思考未來 6G 網路能支援差異化、客製化的 AI 能力和服務應用，以支援對於以 AI 為基礎的新興商業模式及應用。

本團隊藉由蒐集研析 AI-Native 6G 和 Cloud-Native 6G 之跨領域應用情境參考架構，探討 2 種架構在不同應用場景運作和特徵，發現此 2 特徵是相輔相成的面向。Cloud-Native 強化運作於 6G 上各種軟體的安全性，其中也包含各種 AI-Native 的應用，不易被惡意攻擊。而 AI-Native 提升網路服務效能以及降低能耗，提升 Cloud-Native 的運作效能，強化以 Cloud-Native 為基礎的 NFV 解決方案，促進此一型態網路服務的可用性，更加落實未來 6G 的願景以及優勢。

一、SCIL—創新系統架構，無縫接軌未來 6G 應用

在實證階段，本計畫建立跨領域應用雛型系統的基礎環境設定，並詳細說明實證效果，藉此驗證建立的參考架構之可行性與效能，為未來 6G 網路應用實現提供指引。本計畫設計了 SCIL 系統，包含開

發一 APP 及改善 COIL 演算法。使用者可以藉由 APP 方便地應用和管理模型，並擁有易於使用的介面。「模型應用」功能讓使用者可以輕鬆進行圖片預測，「新資料上傳」功能為模型訓練提供清晰的工作流程，並能夠迅速反映訓練狀態。最後，「產品內容」功能提供快速查看可辨識商品類別的選項。演算法修改部份除了藉由實現類別數的靈活設定，從而允許在不同時間點新增不同數量的類別，使其更符合 6G 實際應用需求外，也縮短訓練時間，這對於需要快速上架新品項的智慧商店等應用場景非常重要。

二、智慧商店實證，根據應用需求選擇最佳模型

實證部份則是實際使用智慧商店的商品圖片比較 CNN 和 CIL 2 種模型在多個任務中的性能表現，以評估它們在 6G 跨領域應用中的適用性。結果顯示，CNN 在處理新類別時有較高的準確率和較短的訓練時間，但對舊類別的準確率較低，而 CIL 在各個任務中都能夠維持相對穩定的正確率，但需要較長訓練時間。根據不同應用場景的需求，可以選擇適合的模型，以取得最佳性能和效能。此研究為 6G 應用領域提供重要參考，幫助選擇適合的 ML 模型以實現不同的辨識需求。

三、科技發展建議，促進 6G 跨領域應用的實現和推動

- (一)鼓勵跨領域應用研究：建立跨領域應用的政策指引，鼓勵與支持各行業之間的合作，以及推動創新和技術整合，進一步促進未來 6G 網路應用發展。
- (二)推動數位轉型：支持企業和組織進行數位轉型，如實體零售中的智慧商店，透過政策支持，提供相應資源和指導，幫助業者採用先進的技術，從而提升效率、創造價值。
- (三)促進創新科技研發：透過政策投資和支持，確保具有前瞻性的科技基礎建設，如 6G 通信技術、機器學習平臺等，能夠迅速發展與應用於商業領域。



(四)資料隱私和安全政策：為了建立可信賴的 6G 應用環境，應制定和實施嚴格的資料隱私和安全政策，以保護個人和企業的資料安全。

第三章 規劃與建立安全與可靠的 6G 跨領域應用機制與技術

先導評估

ITU-R M.2410^{3.1} 提出 eMBB、mMTC 和 uRLLC 等 5G 的主要應用場景。其中，eMBB 用戶面延遲為 4 ms，下行數據速率達 20 Gbps，uRLLC 所需的用戶面延遲為 1 ms，需要每平方公里能夠支持 106 部設備。而 6G 在 5G 基礎上，進一步拓展到支撐高效能、高密度、廣域覆蓋之無線網路，從毫米波頻段擴展到太赫茲 (THz) 頻段以最大限度提高容量增益，網路營運商須布建更多基地臺等硬體設備以達相同覆蓋率，導致網路布建成本增加。此趨勢致使國際標準組織採用網路虛擬技術支持多租戶情境，讓營運商可將網路元件部署於白牌伺服器以提高服務靈活性及降低成本。但虛擬主機效能比不上專有硬體主機，需要最佳化虛擬網路元件以確保性能和服務品質 (Quality of Service, QoS)，網路營運商將難滿足可靠性、品質及可用性^{3.2、3.3、3.4}的需求。為此，本章評估結合邊緣運算與 BC 來建立去中心化的管理機制與分散式資料儲存系統之可行性。

本章首節對大量 IoT 裝置下，研析強化服務韌性的容錯技術，及各國際組織的公布白皮書及相關文件，其 MEC 及 DLT 的技術規範，以建立資料分享機制。由於國際組織定義的邊緣運算技術皆使用虛擬技術，在此先介紹現行的虛擬技術，技術項目如下：

- (一) NFV 將網路功能拆分成不同的虛擬元件。以 Docker 為例，網路功能被封裝成容器元件，再以容器編排 (Container Orchestration) 技術部署與管理。

3.1 [ITU-2410] Minimum requirements related to technical performance for IMT-2020 radio interface(s), 2017 report, Retrieved from <https://www.itu.int/pub/R-REP-M.2410>

3.2 [RFC-1] Network virtualization research challenges, <https://datatracker.ietf.org/doc/html/rfc8568>

3.3 R. Glitho Cloudifying the 3GPP IP multimedia subsystem: why and how? 6th International Conference on New Technologies, Mobility and Security (NTMS) (2014), pp. 1-5 Google Scholar

3.4 [RFC-2] Multi-domain Network Virtualization. Retrieved from <https://www.ietf.org/archive/id/draft-bernardos-nfvrg-multidomain-00.txt>

(二) 虛擬網路技術，在實體網路創建彼此隔離的虛擬網路，目前較複雜的技術為 SDN 可提供虛擬交換器功能，提供一般元件的網路連結，而目前坊間的容器編排工具也提供虛擬網路建置工具提供容器間的連結，但對象只限於編排工具產生的容器。

(三) MEC 編排器 (Multi-access Edge Computing Orchestration, MEO)，邊緣運算之網路元件及資源之編排工具，負責邊緣運算環境虛擬環境建置。

(四) 虛擬化網路元件的監督技術，用於觀察網路元件狀態，可以由容器編排工具提供的容器介面組成。

除此之外，IDC 預測^{3.5}到 2025 年將有 1500 億個邊緣和 IoT 相關設備被部署。國際顧能有限公司 (Gartner) 也預計^{3.6}，由於 IoT 的擴展，到 2025 年 75% 的企業生成數據將在傳統數據中心或雲端之外建置和處理。因此，第二節將分散式 IoT 系統以虛擬化技術部署在邊緣運算架構進行評估效能及可行性。

國際組織多建議以 DLT 來建構新型態的安全架構及分散式儲存系統，但這樣的趨勢還處於發展初期，許多標準尚未制定完成，已發表的技術文件也須整合測試。因此第三節的應用情境實證將整合 BC、MEC，發展用於 IoT 應用情境的去中心化資料分享平臺，以驗證上述研析之標準結合後的可行性。

3.5 Raghbir Singh, Sukhpal Singh Gill. (2023) Edge AI: A survey. Retrieved from <https://www.sciencedirect.com/science/article/pii/S2667345223000196#bbib72>

3.6 Gartner. (2018) Retrieved from <https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders>

第一節 發展容錯技術強化服務韌性

感知能力將是行動通訊系統在 6G 時代能提供的重要能力之一，數以億計的 IoT 裝置收集各種資料，提供公司或組織對各種事件做成決策，與現行企業專網架構類似。就目前收集的資料得知，國內部分電信業者推行的方案都類似台灣大哥大的合作廠商瑞擎數位 MEC Gateway，仍使用遠端認證撥接使用者服務(Remote Authentication Dial In User Service, RADIUS)這種中央式認證機制，如圖 32 所示，進而推論國內還未有將分散式系統架構於 MEC。

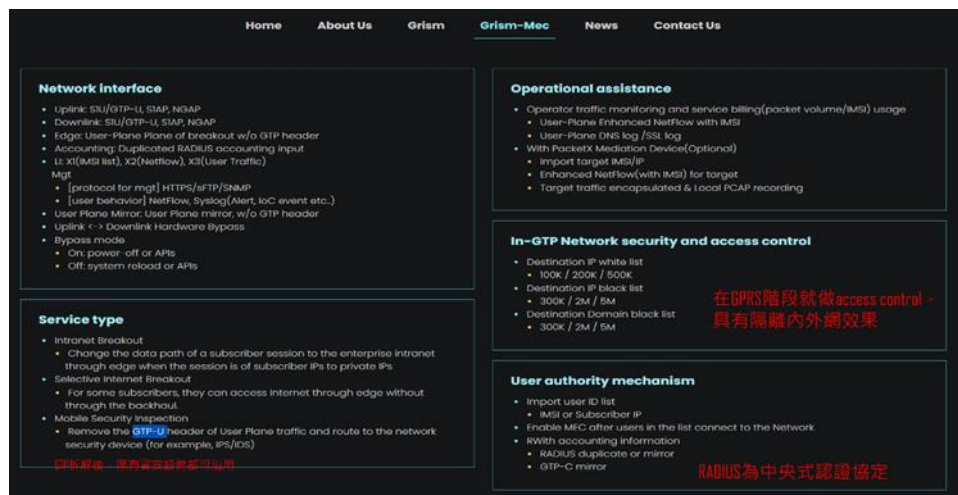


圖 32、瑞擎數位 MEC 閘道器規格

資料來源：瑞擎數位^{3.7}

中央式認證機制所產生的延遲，即使用戶就近使用跨電信營運商的網路服務，也無法達到電信網路的服務品質。尤其當服務架構在基於 NFV 技術的網路環境，需要跨營運商之資料分享機制以掌握整體網路狀況，提升網路服務品質。因此，無需事先有信任關係即可共享網路資源，僅將服務系統以分散式方式建置，將可提升網路服務的容錯能力。

3.7 GRISM-MEC. (2023) Retrieved from <https://packetx.biz/zh/products-grism.php> (Jul. 03, 2023)

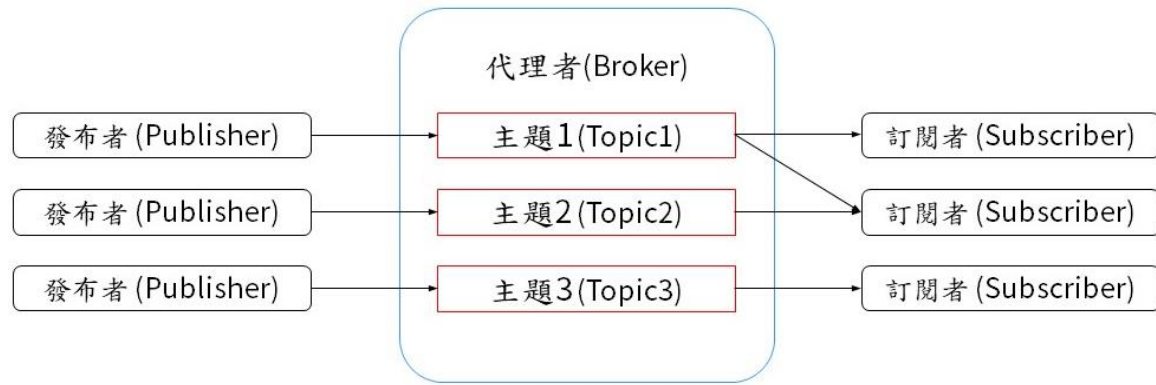
針對 IoT 網路服務建置已有一些標準及研究論文提出解決方案，本節將整理相關標準、論文及開源計畫，重點方向涵蓋「IoT 部署於邊緣運算環境架構」、「DLT 之去中心化認證架構及儲存系統」及「IoT 運作協定及相關容錯機制」。

一、IoT 部署於邊緣運算環境架構

(一)IoT 協定

IoT 本質即是裝置，而連上網的目的就是要做運算，最後將運算結果回饋到提供服務的伺服器。由於 IoT 裝置規格多變，運算能力、連線能力及儲存能力也各有不同，因此前述的服務伺服器通常不會直接連線 IoT 裝置，而是透過代理者(Broker)，以圖 33 訊息佇列遙測傳輸(Message Queuing Telemetry Transport, MQTT)之 IoT 協定為例：

1. 訂閱者(Subscriber)是提供服務的伺服器，會向 Broker 訂閱指定的主題(Topic)。
2. 發布者(Publisher)是 IoT 裝置，會向 Broker 發布特定的主題(Topic)。
3. Broker 會判斷 Publisher 發布的主題是否被 Subscriber 所訂閱，如果有訂閱，便將此 Topic 的訊息傳送給 Subscriber。

**圖 33、MQTT 協定示意圖**

資料來源：請參閱附錄-參考資料^{3.8}

(二) 早期 IoT 容錯機制

IoT 裝置的運算能力、連線能力及儲存能力各有不同，早期 IoT 系統無統一的通訊協定，但也會設計一個能力較好的節點，除執行 Broker 工作外，也會當成容錯機制的節點。容錯機制包括資料複製 (Data Replication) 及服務系統備援 (Service Redundancy)，如透過^{3.9}、^{3.10} 設計一些可區別之儲存節點 (Distinguished Storage Nodes) 用於收集儲存單一 Topic 的資料，同時複製副本到鄰近節點，達成服務系統備援。針對複製的方法，結構化資訊標準促進組織 (Organization for the Advancement of Structured Information Standards, OASIS)^{3.9} 提出動態複製方法，副本在預定範圍內隨機放至其他節點，其中副本數 (Replica Number) 在此論文被最佳化，其中最佳化方式是當副本要更新時，根據預定範圍內的節點密度，決定複製節點數量，同時複製節點使得副本分布更加隨機，作者以實驗驗證此

3.8 K. Piotrowski, P. Langendoerfer, and S. Peter. (2009). "tinyDSM: A highlyreliable cooperative data storage for Wireless Sensor Networks," in 2009 International Symposium on Collaborative Technologies and Systems, pp. 225–232, Ieee, 2009.

3.9 Richard Copen, Andrew Banks, Ed Briggs, Ken Borgendale, Rahul Gupta (2019) MQTT Version 5.0. Retrieved from <https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.pdf>.

3.10 S. Ratnasamy, B. Karp, L. Yin, F. Yu, D. Estrin, R. Govindan, and S. Shenker. (2002) "GHT: A Geographic Hash Table for Data-Centric Storage," in Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications (WSNA '02), vol. 5, pp. 78–87, ACM, 2002.

機制可達成較好的容錯能力。另一種選擇副本動態複製方法^{3.11}，副本要存放於哪一個 IoT 裝置，是由幾個 IoT 裝置資源的評分系統決定，其中 IoT 裝置資源包括 RAM、電力及通訊範圍，同時提供針對系統資源特徵之自我檢查機制，可重啟失效的系統，但此機制並不考慮用戶特定的容錯需求。隨著技術發展，IoT 應用系統不再是裝置廠商自行定義通訊協定的封閉產品，國際商業機器公司 (International Business Machines Corporation, IBM) 等業者提出 Publish/Subscribe IoT 通訊協定，如圖 33 的 MQTT Broker 節點，在一般的應用中，Broker 節點是資源較多的節點，因而被當成副本的存放節點，在此情況下，就不須額外設計容錯機制，只要將資料複製到 Broker 就可達成系統備援的目的。

(三)IoT 部署於邊緣運算環境

早期的 IoT 相關論文並未考慮大範圍部署，如上所論述的解決方案皆以自行架設網路或模擬的網路進行探討。因此，當 IoT 設備要部署到 6G 行動網路，就必須考慮 IoT 運算建立於雲端運算架構或是邊緣運算架構的優缺點。雲端運算是基於資源豐富中央機房，主要的優點是有無限的儲存容量及運算資源，但也面臨集中式系統單點失敗、較慢的服務速度及連接速度等問題，當 IoT 系統架構在雲端運算架構將有高延遲及低可靠的效能表現。為此，學界/業界提出邊緣運算架構，將計算及儲存空間向用戶的行動裝置接近，以滿足 6G 行動網路所提的低延遲及高可靠等關鍵績效指標。

(四)ETSI 的 MEC 技術

為了評估 IoT 應用系統架構在 5G/6G 環境的可行性及效能，將就 ETSI 的 MEC 技術(ETSI-MEC)進行說明，包含 ETSI-MEC 系

3.11 J. Neumann, N. Hoeller, C. Reinke, and V. Linnemann. (2010) "Redundancy Infrastructure for Service-Oriented Wireless Sensor Networks," in 9th IEEE International Symposium on Network Computing and Applications (NCA 2010), pp. 269–274, IEEE Computer Society, July

統簡介，MEC 相關應用情境及現行 IoT 應用在 MEC 的部署案例。與其他標準比較，ETSI-MEC 的技術內容最全面，明確指出 MEC 伺服器將有較好的儲存能力以及計算能力，並可與其他 MEC 伺服器組成 MEC 叢集(MEC Cluster)，即可在 MEC 環境架設分散式系統。

1. ETSI-MEC 系統簡介

首先，以 ETSI 發布的白皮書及標準^{3.12}，探討邊緣運算如何就近完成用戶要求的工作，由於邊緣運算架構不斷演進，現有行動系統網路包含雲端、霧、邊緣等運算架構，如圖 34 所示。

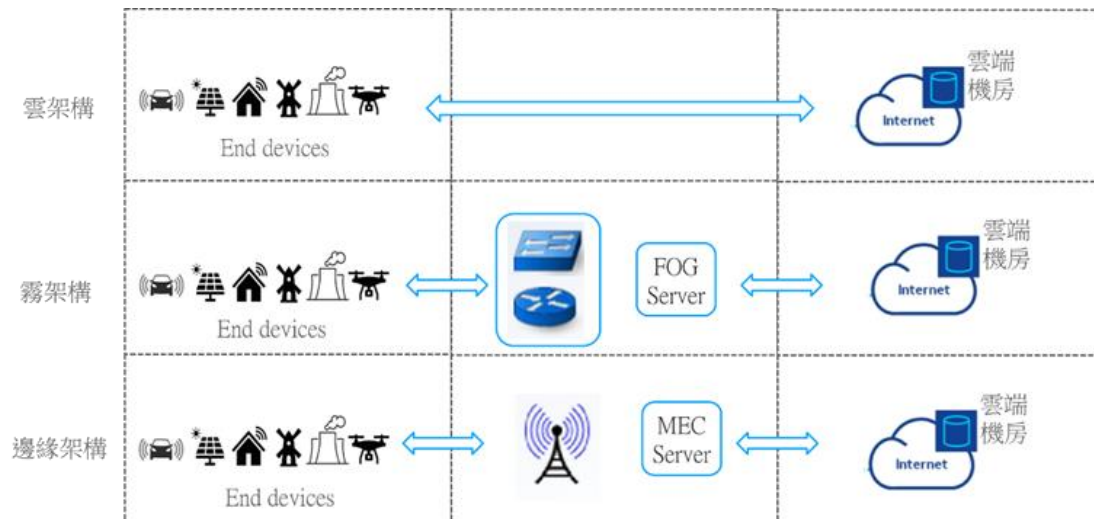


圖 34、雲端、霧、邊緣運算架構演進示意圖

資料來源：請參閱附錄-參考資料^{3.12}

在雲端運算架構中，行動裝置將資料經過核心機房上傳到雲端，使得大多數計算發生在雲端，而霧運算架構則在終端和雲端資料中心之間再加一層帶有路由器、交換器及伺服

3.12 Yun Chao Hu, Milan Patel, Dario Sabella, Nurit Sprecher and Valerie (2015). Mobile Edge Computing A key technology towards 5G Retrieved from https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

3.12 Yun Chao Hu, Milan Patel, Dario Sabella, Nurit Sprecher and Valerie (2015). Mobile Edge Computing A key technology towards 5G Retrieved from https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

器，把一些資料在這一層直接處理和儲存，以減少雲端資料中心壓力，提升整體運算架構的效能。最後的行動邊緣運算 (Mobile Edge Computing) 架構，則是將伺服器放在基地臺旁邊，與霧運算架構相同，會留下一些資料直接處理和儲存，但比霧運算架構更接近終端用戶。而如何就近提供用戶運算與儲存資源，可以在 ETSI 2014 年發表的白皮書^{3.13} 發現最終目的即是降低延遲，盡可能提升行動網路吞吐量。經過幾年的演進，ETSI 將 MEC 從原先的 Mobile Edge Computing 改成 MEC 架構，即是在基地臺附近將數據分流，讓特定應用的資料不須經過核心機房就可到達目的地。如企業專網的邊緣運算架構會比霧運算架構還具彈性，也是目前各個國際標準及論文討論的對象，如圖 35 所示。

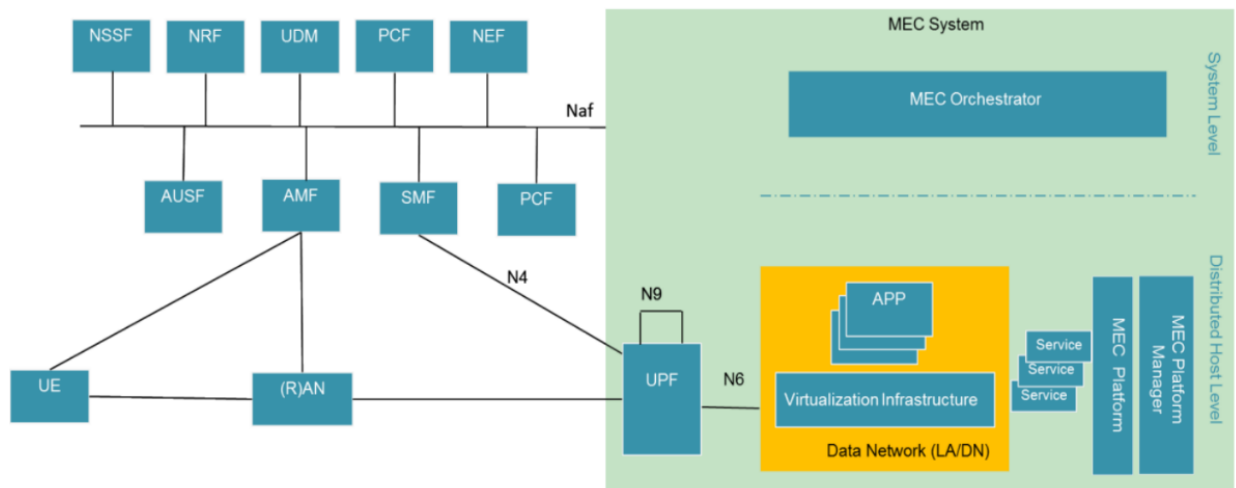


圖 35、MEC 示意圖

資料來源：請參閱附錄-參考資料^{3.14}

3.13 ETSI. (2015). Mobile-Edge Computing Retrieved from https://portal.etsi.org/portals/0/tbpages/mec/docs/mobile-edge_computing_-_introductory_technical_white_paper_v1%2018-09-14.pdf

3.14 Adopting Multi Access Edge Computing (MEC) into 5G Networks. Retrieved from <https://www.hsc.com/resources/blog/adopting-multi-access-edge-computing-mec-into-5g-networks/> (Jul. 03, 2023)

行動網路的運算架構不斷演進，目前的邊緣運算架構邊緣伺服器架設基地臺旁邊，使用連結管理功能（Session Management Function, SMF）及使用者平面功能（User Plane Function, UPF），將部分雲端運算平臺上的服務資源卸載至邊緣運算架構當中，以改善應用服務用戶之延遲體驗。當資料從 UPF 被導入邊緣運算環境，MEC 主機層（Host Level）會有對應的應用程式或服務處理，而應用程式或服務則由系統層（System Level）的編排器（Orchestrator）以虛擬基礎建設（Virtualization Infrastructure）生成，ETSI^{3.12,3.15} 同時增加 MEC 的儲存能力以及運算能力，並假設 MEC 內部的資源服務有一個編排器進行管控虛擬基礎建設，形成一個 MEC 系統。MEC 系統可透過網路元件虛擬化技術，如 SDN、NFV，與其他 MEC 系統/核心網路進行協同合作，來支撐起多元服務的 B5G/6G 網路架構。

由上面論述的運算架構演進過程得知，IoT 運算架構會影響營運韌性。當運算發生在中央式資料中心與 IoT 裝置之間，則存在集中式系統常有的單點失敗問題，同時資料經由電信公司中央機房傳到資料中心後，運算結果再回傳裝置，將產生延遲，使得 IoT 系統逐漸移向邊緣運算環境。

3.12 Yun Chao Hu, Milan Patel, Dario Sabella, Nurit Sprecher and Valerie (2015). Mobile Edge Computing A key technology towards 5G Retrieved from https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf
3.15 Sami Kekki, Walter Featherstone, Yonggang Fang, Pekka Kuure, Alice Li, Anurag Ranjan, Debashish Purkayastha, Feng Jiangping, Danny Frydman, Gianluca Verin, Kuo-Wei Wen, Kwihoon Kim, Rohit Arora, Andy Odgers, Luis M. Contreras, Salvatore Scarpina. (2018) MEC in 5G networks. Retrieved from https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

2. 單一場域 IoT 應用於 MEC

就單一場域的 IoT 應用，Broker 可以安裝在 MEC，藉由邊緣運算環境完成與 IoT 裝置的運算溝通，可緩解前述單點失敗及較大延遲 2 個問題，同時得到效益如下：

- (1)降低 IoT 裝置與內部網路之間的延遲，提供更高的營運效率。
- (2)資料不需一路傳到中心機房，頻寬使用率相對較低。
- (3)即便系統失去與雲端的連接，IoT 裝置運算仍可進行，提高營運韌性。

在 ETSI 的白皮書^{3.12}也建議將 IoT 閘道器建置於 MEC 服務器上，如圖 36 所示。閘道器是用來聚合 IoT 裝置在行動網路上產生的訊息，一般來說，這些訊息都很小，經過加密，並且採用不同形式的協議，需要一個低延遲聚合點來管理各種協議、消息分發和分析處理。當 IoT 閘道器部署於 MEC，部分數據可以就近由閘道器的應用程序處理，減少數據經由核心機房(Mobile Core)到雲端資料中心的往返時間，可以滿足某些連接設備需要即時功能的性質。

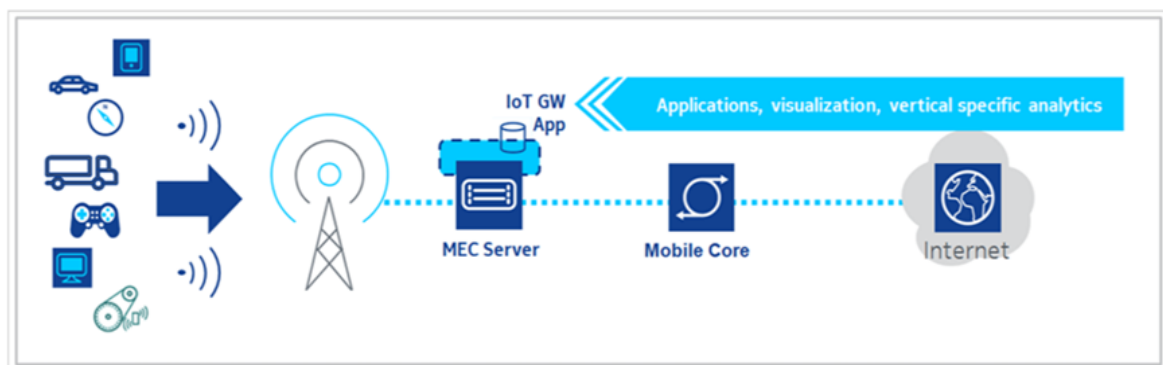


圖 36、MEC IoT 應用場景

3.12 Yun Chao Hu, Milan Patel, Dario Sabella, Nurit Sprecher and Valerie (2015). Mobile Edge Computing A key technology towards 5G Retrieved from https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

資料來源：請參閱附錄-參考資料^{3.12}

除此之外，ETSI 白皮書^{3.16}也建議使用 MEC 伺服器提升內容遞送網路(Content Delivery Networks, CDN)效能，也就是在 MEC 上建立本地快取(Local Cache)機制，配合 CDN 在核心機房原有的快取(Central Cache)，提升行動用戶裝置的吞吐量，如圖 37 說明 MEC 可以擴展原有網際網路的 CDN 功能到行動網路，提升行動用戶體驗成效。

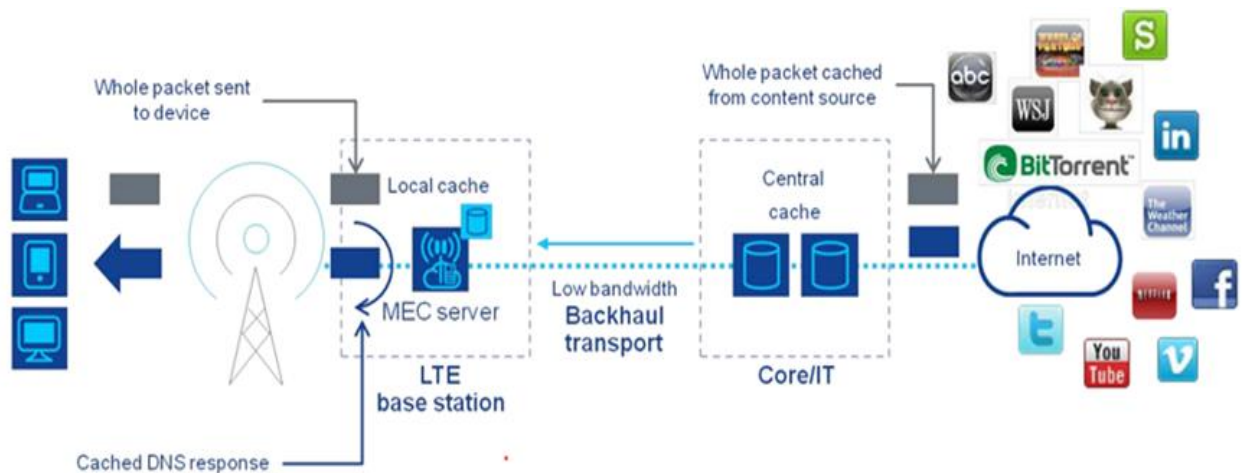


圖 37、MEC CDN 快取機制

資料來源：請參閱附錄-參考資料^{3.16}

3. 現行 IoT 應用在 MEC 的部署案例

上述 2 個 ETSI 早期提出的 MEC 應用場景，在單一場域應用確實可以達成減少傳輸延遲、增加網路吞吐量。但由於早期的 MEC 強調的是 Mobile Edge Computing，並未配置移動接入點，即是基地臺轉發流量。許多資料還是需要經過核心機房到雲端資料中心或公司內部，無法真正地減少傳輸延遲、增加網路吞吐量，也許這樣的原因，ETSI 將 MEC 定義為 Multi-access Edge Computing，開始規範多接入邊緣運

3.16 ETSI. (2015). Mobile-Edge Computing Retrieved from https://portal.etsi.org/portals/0/tbpages/mec/docs/mobile-edge_computing_-_introductory_technical_white_paper_v1%2018-09-14.pdf

算標準，使得現行國際標準的 MEC 變成如圖 35 所示的架構，而應用場景則如圖 38 所示。

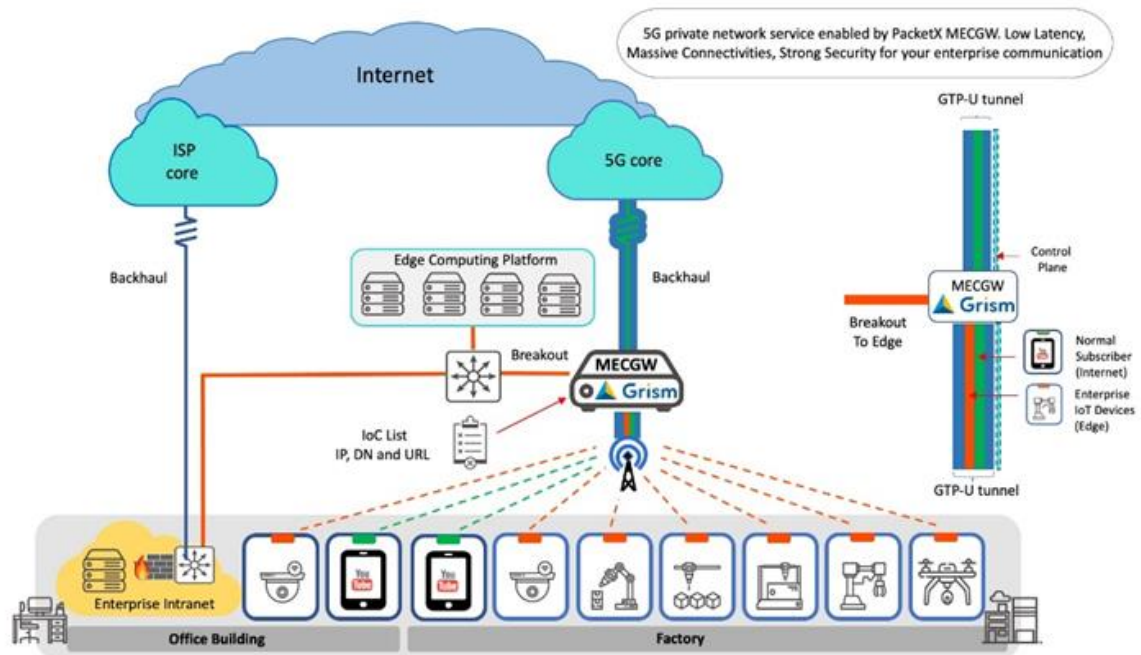


圖 38、MEC IoT 應用場景

資料來源：請參閱附錄-參考資料^{3.7}

MECGW 為 MEC 閘道器，資料收集及處理後，便從基地臺轉發到企業內部，即使有多個 IoT 應用場域，也不會消耗核心網路的頻寬。現行的 MEC 閘道器除了基地臺轉發功能，同時增加 MEC 的儲存能力以及計算能力，使得邊緣運算架構包含 4 種參與者：

- (1) 在辦公室 (Office Building) 或工廠 (Factory) 用戶設備 (User Equipment, UE) 連上行動網路，讀取 IoT 裝置資訊。
- (2) 行動網路業者 (Operator) 設置、維護 MEC 閘道器 (MECGW)，為 MEC 的擁有者。
- (3) 網際網路提供商 (Internet Service Provider, ISP)，提供企業內網 (Enterprise Intranet) 與 MEC 閘道器轉發點的連線。

3.7 GRISM-MEC. (2023) Retrieved from <https://packetx.biz/zh/products-grism.php> (Jul. 03, 2023)

(4)應用服務提供商，提供應用程式在 MEC 閘道器上執行。

4 種參與者將共同運轉邊緣運算架構，建構低延遲、高吞吐量的 6G 行動網路，同時促進全新服務的開發。

二、DLT 之去中心化認證架構及儲存系統

各國及各大廠對 6G 所提需求如超高速、低延遲等，將導致各電信業者在技術規格要求及成本考量下，逐漸走向電信基礎建設分享及多租戶等新型商業模式。伴隨這些模式，現有邊緣運算架構的安全及信任模型不足以對應，攻擊者有機會透過資源共享相關漏洞進行針對其他租戶的橫向移動(Lateral Movement)，進而干擾電信服務及基礎建設資源。隨著趨勢的擴展，各國標準組織逐漸將共享資料、新的安全及信任框架作為發展目標。

就目前相關的國際標準及論文，討論 5G/6G 的安全及信任框架，如上一小節所述，目前只有 ITU 的已提案討論群組建議將 BC、IoT 及 MEC 結合^{3.17}，以及 ETSI 的群組報告(GROUP REPORT^{3.18})討論如何使用 BC 在邊緣運算環境管理資料，因此下面論述的文件 BC 並沒有明確指出架設在 MEC 系統。

(一)ETSI 相關標準

首先以圖 39 介紹 BC 工作流程：

1. Initiating Transaction：任何註冊到 BC 系統的參與者都會得到私鑰(PrivateKey)，參與者要發起交易，會使用 PrivateKey 對交易產生數位簽章用，來證明發起交易的參與者身分。

3.17 ITU_Y.4486. (2023) Framework of cross edge decentralized service by using DLT and edge computing technologies for IoT devices. Retrieved from <https://www.itu.int/rec/T-REC-Y.4486>

3.18 ETSI GR PDL 009 V1.1.1 (2021-09) Permissioned Distributed Ledger (PDL); Federated Data Management.

https://www.etsi.org/deliver/etsi_gr/PDL/001_099/009/01.01.01_60/gr_PDL009v010101p.pdf

2. Broadcasting and Verifying Transactions：發起交易的參與者對所有 BC 節點廣播，BC 節點使用公鑰(Public Key)及數位簽章驗證參與者身分。
3. Building New Block：所有 BC 節點建立區塊(Block)，開始使用共識協定流程。
4. Validating New Blocks base on a Consensus Protocol：所有 BC 節點使用共識協定演算法計算，最後只有一個 BC 節點可獲准寫入 BC。
5. Updating Blockchain：獲准寫入的 BC 節點更新 Block 到主鏈。

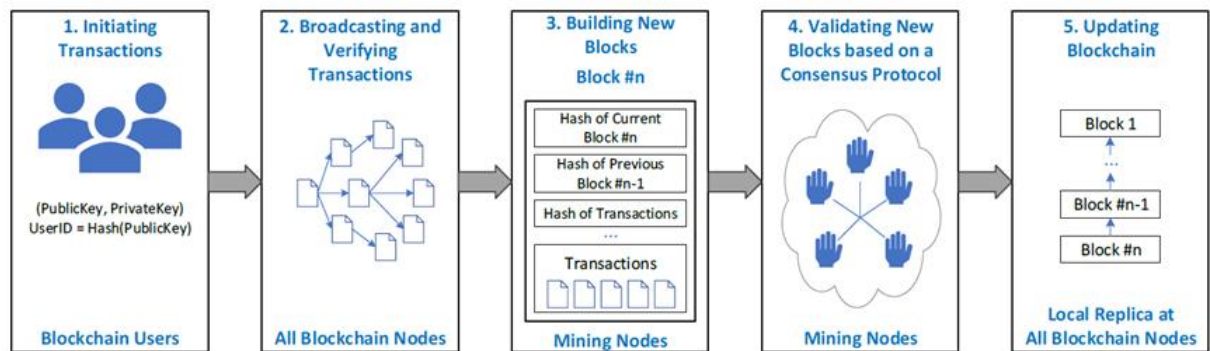


圖 39、BC 工作流程

資料來源：請參閱附錄-參考資料^{3.19}

BC 是一種 DLT 技術，在圖 39 的步驟 1 的數位簽章只是驗證身分，讓參與者無法否認發起交易，真正的安全是建立在共識流程，只有在步驟 4 取得其他 BC 節點共識，才能寫入 BC，即是完成交易。而此工作流程對任何參與者發起交易都不會不同，也就是對任何參與者不存在任何事先的信任。除此之外，ETSI 的群組報告^{3.18}

3.19 Chonggang Wang (Lead), Mischa Dohler, Diego R. López, Raymond Forbes, Shahar Steiff, Tooba Faisal, Sheeba Backia Mary B., Qianren Liu, Ismael Arribas. (2022). An Introduction of Permissioned Distributed Ledger (PDL) Retrieved from <https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP48-PDL.pdf>

3.18 ETSI GR PDL 009 V1.1.1 (2021-09) Permissioned Distributed Ledger (PDL); Federated Data Management. https://www.etsi.org/deliver/etsi_gr/PDL/001_099/009/01.01.01_60/gr_PDL009v010101p.pdf

建議資料儲存、分享及計算都留在邊緣環境的管理架構，並討論使用 DLT 在各方參與者間建立信任關係，同時也指出當 AI 運算的輸入資料來自於不同組織，基於 DLT 的資料管理架構可以緩解各組織間如何建立信任關係的問題，但是有效率的存取資料則須解決。

關於以 DLT 架構的標準，由於大多數的標準組織都還在持續進行中，如圖 40 所示的程式架構，由多個標準文件及論文組合，各單元介紹如下：

1. BC App：會被部署到 BC 的區塊，每當 User 發起交易就會執行區塊中的程式碼，由於區塊會被每個節點所保存，故以去中心化應用程式(Decentralized Application, dApp)標示。在此參考架構，User 發起交易透過 dApp 存取 BC 資料。
2. BC Platform：提供介面讓 dApp 呼叫 BC 各種功能。
3. 區塊鏈即服務(Blockchain as a Service, BaaS)：在此參考架構圖的 BaaS 只顯示包裝多種 BC 系統，讓上層的 Blockchain platform 方便呼叫，其他的功能會透過圖 44 說明。
4. open-source BC：包含公鏈(如比特幣)，或是自行架設的私鏈。
5. Off-Chain Storage：鏈下儲存裝置(Off-Chain Storage)配合 BC，用於儲存大型資料。

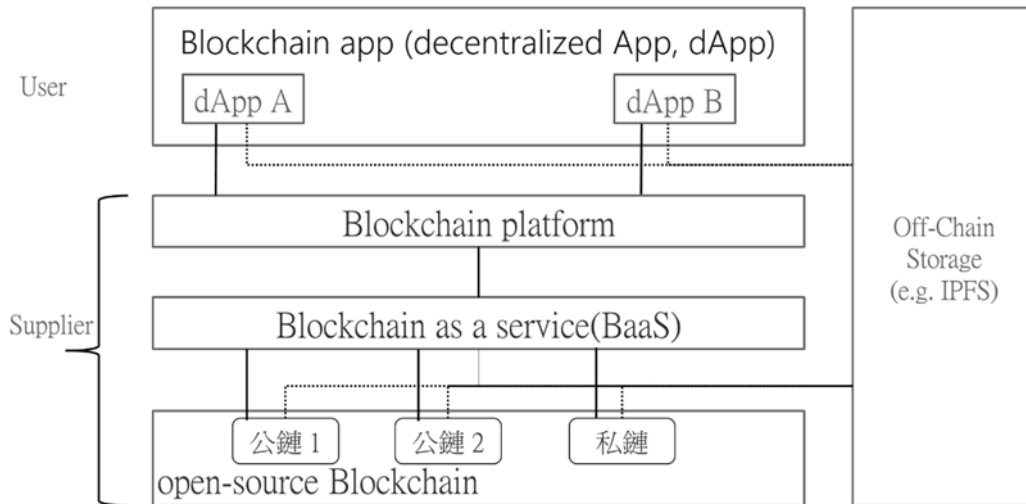


圖 40、DLT 參考架構

資料來源：請參閱附錄-參考資料^{3.19、3.20}

在圖 40 的說明中，所謂 BaaS 包裝不同 BC 系統的意思，就是透過發展 BC 系統互通介面將不同的 BC 系統連結起來，這概念在 ETSI PDL 白皮書^{3.19}及 ITU Y.3530^{3.20}都有論述。其中，ETSI 的 PDL for Supporting Distributed Data Management 草案^{3.21}中定義許可制分散式帳本功能 (Permission Distributed Ledger Function, PDLF) 負責處理不同 BC 系統互通之工作，讓 dApp 可以透過 BaaS 提供的介面函數存取不同的 BC 系統，PDLF 架構如圖 41 所示，PDLF 的工作大致包括以代理者角色轉發不同 BC 系統的訊息、監控 BC 狀態以及跨鏈達成共識等。

3.19 Chonggang Wang (Lead), Mischa Dohler, Diego R. López, Raymond Forbes, Shahar Steiff, Tooba Faisal, Sheeba Backia Mary B., Qianren Liu, Ismael Arribas. (2022). An Introduction of Permissioned Distributed Ledger (PDL) Retrieved from <https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP48-PDL.pdf>

3.20 ITU Y.3530. (2020). Cloud computing - Functional requirements for blockchain as a service Retrieved from <https://www.itu.int/rec/T-REC-Y.3530/en>

3.21 Draft ETSI GS PDL 013 V0.0.1 (2021-12); Permissioned Distributed Ledger (PDL); PDL for Supporting Distributed Data Management (Draft)

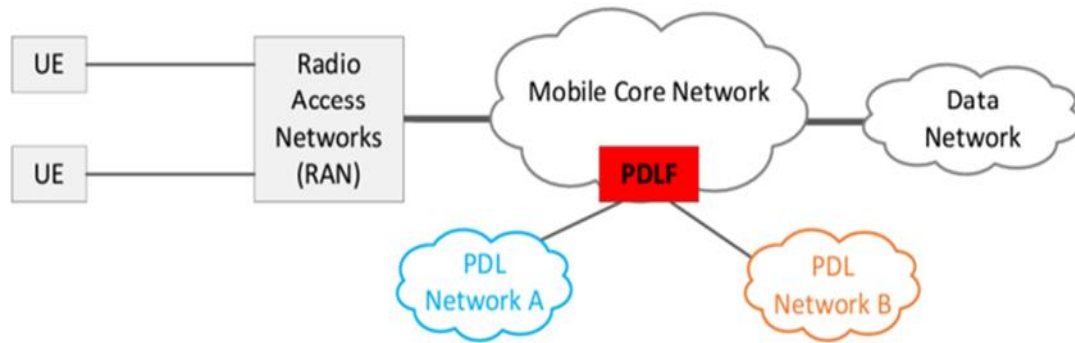


圖 41、PDLF 於行動網路之示意圖

資料來源：請參閱附錄-參考資料^{3.19}

目前以 DLT 建構安全框架的標準組織至少有 ISO、ITU 及 ETSI，其中只有 ETSI 指定使用許可制分散式帳本 (Permissioned Distributed Ledger, PDL)，使用 PDL 好處有：

1. 交易速度快，參與節點須事先認證才可進入，節點數相較於公鏈少，使得交易速度變快。
2. 較好的隱私保護，參與節點教授信任且可控，相較於公鏈可以事後補救機會較大。
3. 交易成本很低，交易不須如公鏈須付費。

當 BC 節點建立在 MEC 服務器上，任何 BC 節點要進入 BC 系統自然需要 Operator 允許，使得 PDL 較符合 MEC 服務器由 Operator 擁有、維護的狀況，同時可以擁有上述優點。但 BC 節點數量太少，有可能會讓某一特定 BC 節點取得 BC 控制權，需要進一步探討。

此外，ITU、IEEE 及 ETSI 同樣使用 DLT 技術建構新的安全框架，只有 ETSI 指定使用 PDL 技術建構私鏈，其他組織則沒有指定，使得部署新的安全框架時，會遭遇公鏈與私鏈的互通問題。但

3.19 Chonggang Wang (Lead), Mischa Dohler, Diego R. López, Raymond Forbes, Shahar Steiff, Tooba Faisal, Sheeba Backia Mary B., Qianren Liu, Ismael Arribas. (2022). An Introduction of Permissioned Distributed Ledger (PDL) Retrieved from <https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP48-PDL.pdf>

就收集到的資料分析，目前似乎還沒有文章討論，而且 BC 技術本身其實還持續演進，使得 BC 互通需持續探討。

(二)ITU 相關標準

ITU 的 DLT 架構標準相似於圖 42，由 Data requestor 輸入資料到 web client (Data sharing platform)，連結到 Ledger node 尋找資料；同時 Data requestor 依照 Data provider 的 Smart contract 處理資料。依據資料的型態，Smart contract 有不同做法：

1. 不含隱私的資料，提供原始資料。
2. 具隱私的資料，只提供分析結果。
3. 動態資料只提供分析結果，Data requester 要提供 smart contract 負責執行分析。

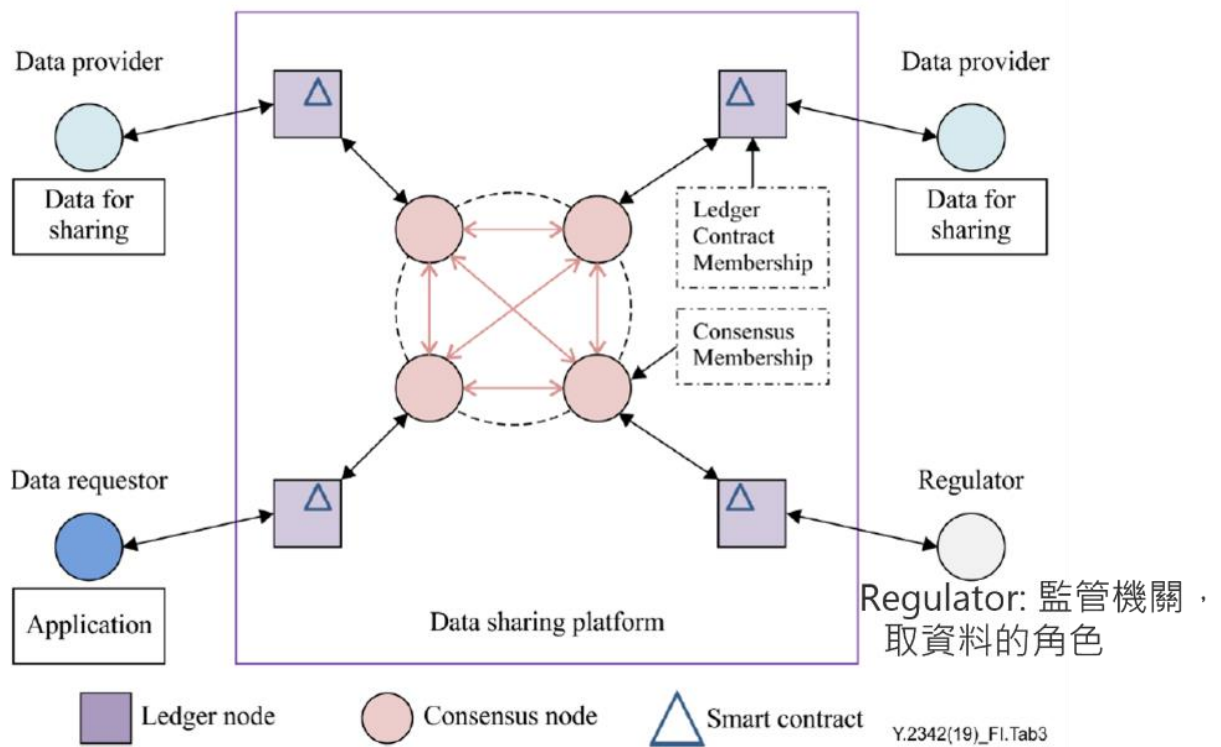


圖 42、BC 資料分享使用例

資料來源：請參閱附錄-參考資料^{3.22}

3.22 IEEE (2020) Standard for Functional Requirements in Blockchain-based Internet of Things (IoT) Data Management. Retrieved from https://standards.ieee.org/standard/2144_1-2020.html.

而圖 43 的步驟則描述加入 BC 如何運作及必要實作的規格：

1. 節點 D 收到參與者發起交易的廣播，節點 D 驗證參與者身分及交易內容。
2. 驗證無誤後，節點 D 就創建一個區塊，再將區塊傳播到所有節點。
3. 節點 A、節點 B、節點 C 檢查區塊的生成證明和所包含交易的有效性。
4. 當驗證無誤，節點 A、節點 B、節點 C 將新區塊添加到鏈尾。

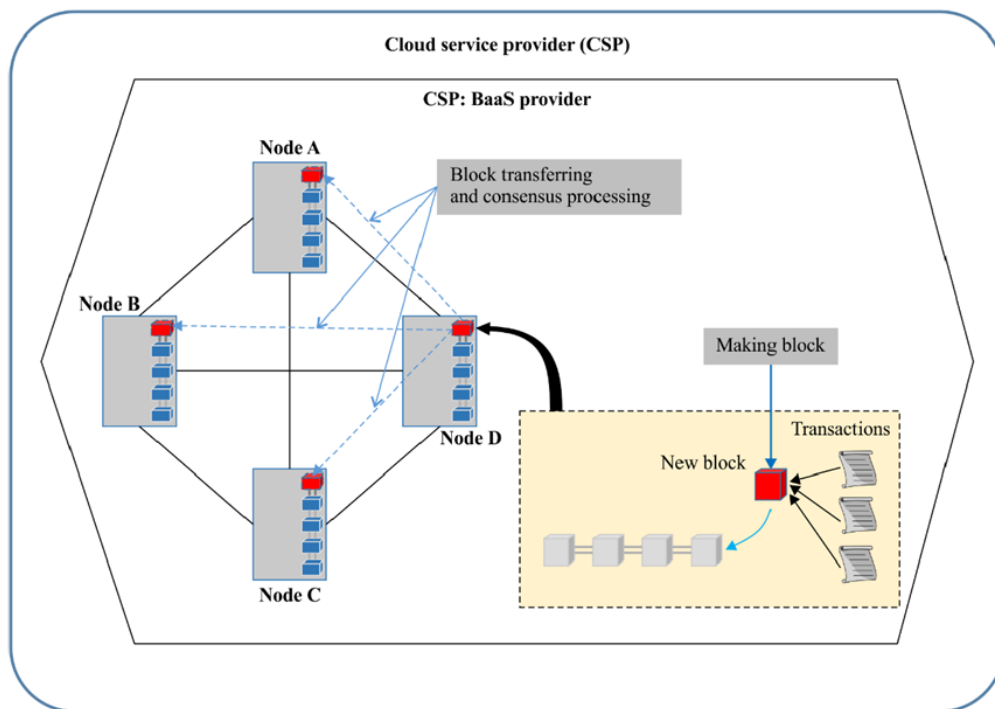


圖 43、BC 加入新區塊過程

資料來源：請參閱附錄-參考資料^{3.20}

這流程假設節點 D 在所有節點參與的共識過程中得到記帳權，一般來說，共識算法應該確保收斂到單一的、不可變的帳本版本。

3.20 ITU_Y.3530. (2020). Cloud computing - Functional requirements for blockchain as a service Retrieved from <https://www.itu.int/rec/T-REC-Y.3530/en>

圖 40 的 BaaS 取自於 ITU^{3.20}，除了上述包裝不同 BC 系統外，還包括提供發展 dApp 的工具包，提供給應用程式開發商。如圖 44 所示的 BaaS 定義於 ITU_Y.3530，在此文件中說明 BaaS 的功能除了提供統一介面管理、使用現行的 BC 系統，還需提供發展工具給應用程式開發商。BaaS 的參與人員包括：

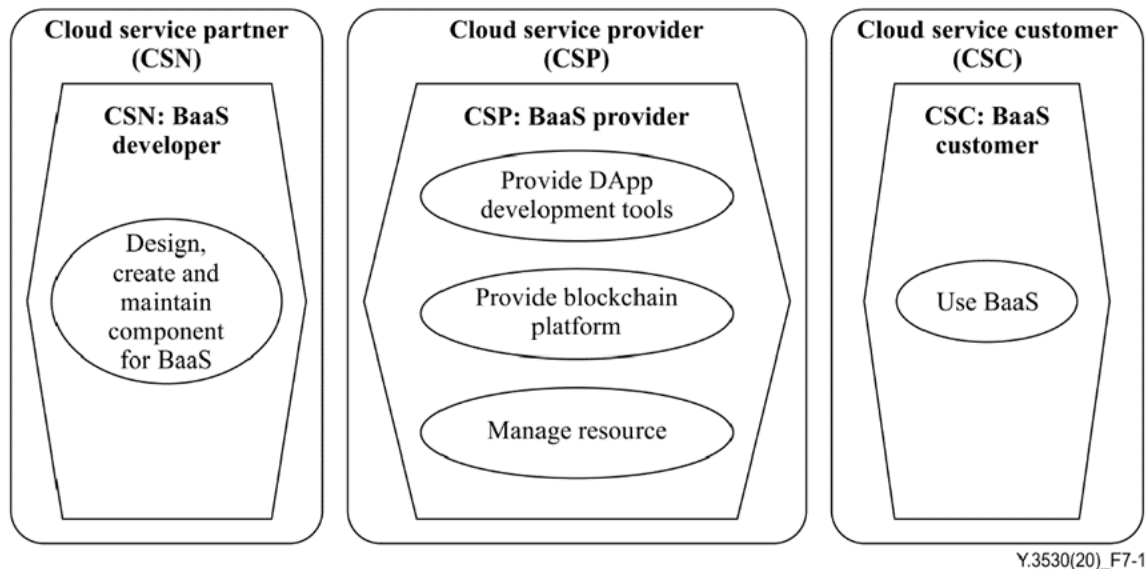


圖 44、BaaS 系統架構

資料來源：請參閱附錄-參考資料^{3.21}

1. CSP 負責建置、營運 BaaS，BaaS 系統包裝現行的 BC 系統並包含 API 給程式開發商開發各種基於 BC 的應用。
2. 雲端服務合作夥伴(Cloud Service Partner, CSN)，使用 CSP 提供的工具，開發 dApp 的應用系統開發商。
3. 雲端服務客戶(Cloud Service Customer, CSC)透過 dApp 使用 BaaS 之行動用戶。

比較圖 40 及圖 44 的人員，圖 40 的 User 相當於 CSC，Supplier 則相當於 CSP，且應該由 Operator 負責營運。除此之外，圖 40 及圖 44 所參考的文件，都是想藉由 DLT 技術建構無需事先有信任關

3.21 Draft ETSI GS PDL 013 V0.0.1 (2021-12); Permissioned Distributed Ledger (PDL); PDL for Supporting Distributed Data Management (Draft)

係即可使用行動網路資源的新型態的安全框架來達成資料共享，而資料共享的目的之一即是最佳化行動網路運作，建立新商業模式，進而符合 6G 關鍵指標。依此推論，DLT 及 MEC 將是 IoT 系統部署需要的技術。

(三)ISO 相關標準

ISO 說明如何建置/使用 BC 標準為 ISO/TR 23455^{3.23}，其他的標準大都進行中。雖然 ISO 有關 BC 標準的推動者為 ETSI，但此標準未明訂以 PDLT 建置 BC，因此，BC 的互通問題須持續注意。

(四)IEEE 相關標準

不同於 ITU 於圖 42 的使用例，IEEE 關於 IoT 資料管理之標準^{3.22}，則建議結合鏈上和鏈下儲存系統發展刪除 API，以達成一些法規要求，如一般資料保護規則(General Data Protection Regulation, GDPR)，即刪除個人資料規定。

實證計畫將結合 DLT、MEC 及星際文件系統(InterPlanetary File System, IPFS)，發展去中心化資料分享平臺。由於自駕車及工廠自動化等應用將引發 IoT 裝置大量成長^{3.24}，如何將大量資料傳回企業或組織內網做後續處理以達成資料驅動型決策的轉型，將是 6G 應用發展的重點之一。因此去中心化資料分享平臺的應用情境將設定資料來自於 IoT，同時提供平臺資料安全、隱私保護及系統容錯等能力，為安全與可靠的 6G 跨領域應用機制之鋪設跨出第一步。

3.23 ISO/TR 23455:2019. (2019). Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems

3.22 IEEE (2020) Standard for Functional Requirements in Blockchain-based Internet of Things (IoT) Data Management. Retrieved from https://standards.ieee.org/standard/2144_1-2020.html.

3.24 徐慶柏, (2023) 【新興領域/2023.05 焦點】2023 年 H1 物聯網領域早期投資觀測：如風嗎？也不如風！. Retrieved from <https://findit.org.tw/researchPageV2.aspx?pageId=2247>

三、IoT 運作協定及相關容錯機制

如前所述，早期的 IoT 系統部署在單一場域，現行協定是發布/訂閱模式如圖 45 所示，只要單純增加備援 Broker 就可完成容錯機制。

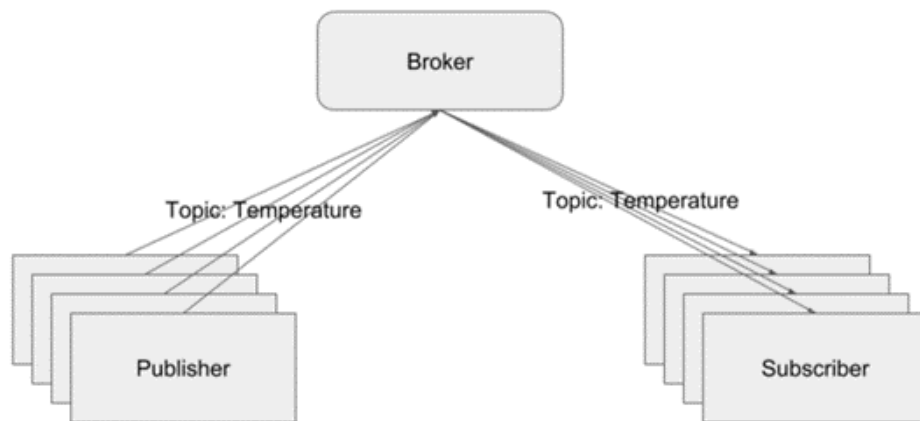


圖 45、發布/訂閱模式示意圖

資料來源：請參閱附錄-參考資料^{3.25}

然而，現有的企業專網應用通常不限於單一場域，可能會橫跨多個基地臺與 MEC 服務器，若單純使用現行發布/訂閱模式協定，如 MQTT，則會如圖 46(a)形成中央式網路架構，產生單點失敗的問題，而圖 46(b)分散式架構，則需考慮安全地複製資料於邊緣以及分享資料給其他 Broker 等問題，將需要進一步設計管理機制。ETSI^{3.11} 使用 Spanning Tree Protocol 建構虛擬區域網路(Virtual LAN, VLAN)以連結不同 MEC 上的 Broker 服務器，並修改 MQTT 的控制訊息，使所有 Broker 可以互傳訊息達成分散式架構的效果，因為 Broker 節點已經可以連結，容錯機制就可直接複製副本在 Broker 節點。

3.25 Gowri Sankar Ramachandran, Kwame-Lante Wright, Bhaskar Krishnamachari. (2018). Trinity: A Distributed Publish/Subscribe Broker with Blockchain-based Immutability Retrieved from <https://arxiv.org/pdf/1807.03110.pdf> (Jul. 03, 2023)

3.11 Yun Chao Hu, Milan Patel, Dario Sabella, Nurit Sprecher and Valerie (2015). Mobile Edge Computing A key technology towards 5G Retrieved from https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

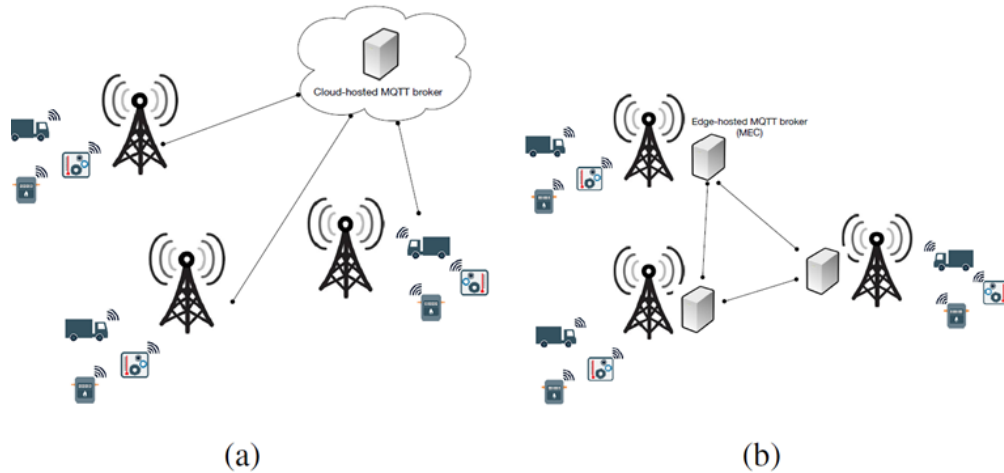


圖 46、中央式代理者結構(a)、分散式代理者結構(b)

資料來源：請參閱附錄-參考資料^{3.26}

若要建置分散式代理者節點的連結除自行建構虛擬區域網路，也可以使用 NFV 技術在 MEC 服務器上建置 Broker 節點，並使用 SDN 技術將在多個 Broker 節點連結起來，而分散式管理機制仍須額外發展，但具有部署彈性、容錯機制較易實施等特性。

就目前收集到的國際標準文件分析，還未收尋到分散式的 IoT 系統相關標準，有關 IoT 系統的標準有 ITU 定義的 Blockchain of Things (BoT)，如圖 47 所示，基於 DLT 技術讓 IoT 系統連結到 BC，即是 BoT，使 BoT 實體，例如 IoT 設備、伺服器、閘道器、服務網閘道器和最終 UE，能夠參與 BoT 並一起進行交易。其中，BoT 實體可以託管一個或多個 BoT 節點和 dApp，BoT 節點透過點對點(Peer-to-Peer, P2P)網路互相通訊，BoT 實體上的 dApp 連接到 BoT 節點以在 BoT 上執行交易。由於 BC 的特性，BoT 在建立信任、降低成本、加速交易以及連接大規模 IoT 設備方面具有優勢。但就如 ETSI 未論述容錯機制相關技術，此文件也未提到分散式代理者管理機制，因此，BoT 比較像是分散式資料儲存及管理系統。

3.26 Edoardo Longo, Alessandro E.C. Redondi, Matteo Cesana, Andrés Arcia-Moret, Pietro Manzoni. (2020) MQTT-ST: a Spanning Tree Protocol for Distributed MQTT Brokers Retrieved from <https://ieeexplore.ieee.org/document/9149046>

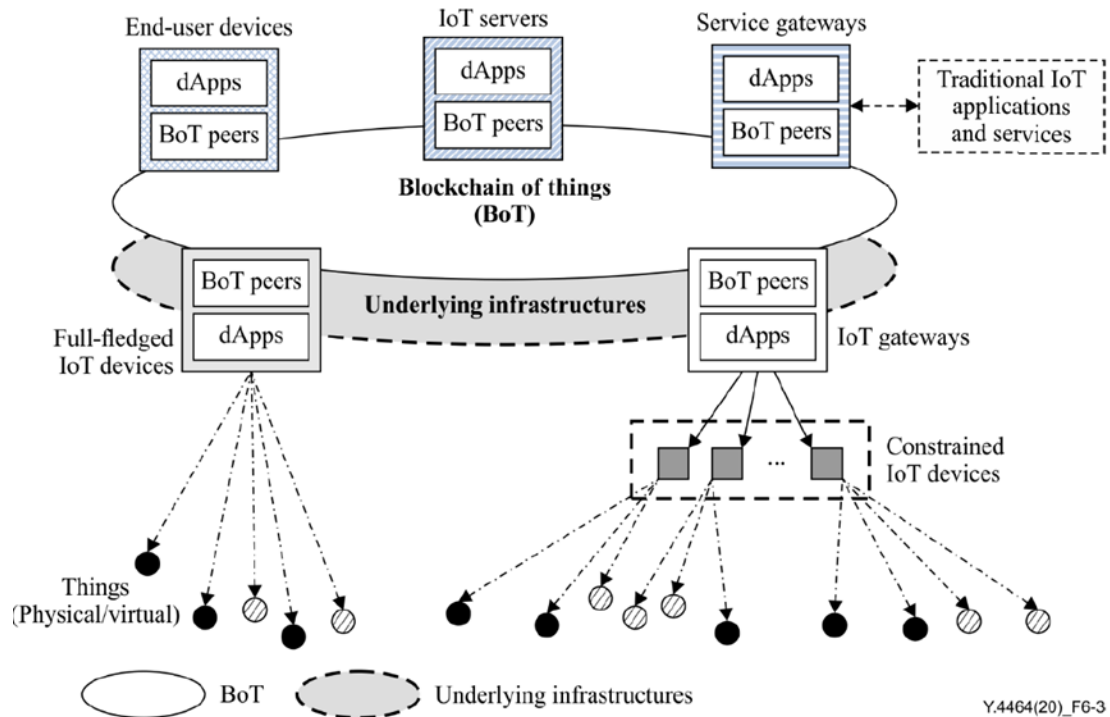


圖 47、Blockchain of Things 概念圖

資料來源：請參閱附錄-參考資料^{3.27}

3.27 ITU-T Y.4464. (2020). Framework of blockchain of things as decentralized service platform. Retrieved from <https://www.itu.int/rec/T-REC-Y.4464>

第二節 分散式及大量裝置(Massive AIoT)的安全議題研析

本節設想情境設定為組織或公司使用第三方提供商或電信業者所提供的 IoT MEC Gateway，以支撐企業內部其他裝置與 IoT 邊緣管理平臺之間的連線。其中 IoT 邊緣管理平臺可以處理來自具有相同管理平臺之身分識別的其他裝置連線，並且在邊緣運算環境中完成所需的運算。為了達成分散式的 IoT 系統，本計畫以 BC 建置去中心化的管理機制，並結合 IPFS 當成鏈下儲存裝置以建置分散式資料儲存系統。然而，在 BC 系統的資料具有不變性，每位使用者可以隨時存取驗證，攻擊者可以取得所有資料分析，將侵害使用者的資料隱私。此外，BC 存在著最長鏈共識，當 BC 系統中出現 2 個版本的 BC，參與者會選擇最長的那一條為準，當惡意參與者控制系統一半以上的計算力，就可藉由共識過程產出最長鏈，將正確的鏈由系統取消，因此如何讓 BC 夠多以避免攻擊，但又不能影響效能，是需要探討的問題。

一、去中心化管理機制研析

在此情境，組織或公司部署橫跨多個基地臺與 MEC 的 IoT 應用，IoT 邊緣管理平臺需滿足下列需求：

(一)去中心化的管理機制

用於管理部署在不同 MEC 的 Broker，如連線狀況監控，提供服務的伺服器的訂閱狀況等。

(二)分散式的資料儲存系統

用於儲存 IoT 裝置發布的資料及資料備援，同時需保持資料的不變性。

(三)去中心化的跨域的認證機制

避免資料被操作篡改，同時避免使用中央式認證機制，以免除單點失敗或較大的延遲。

為滿足上述需求，已經有 Arxiv^{3.25} 及 IEEE^{3.28} 論文使用 BC 機制管理 IoT Broker 節點以及分散式儲存系統，BC 本質是一種 DL，經由密碼學的雜湊函式(Cryptographic Hash Function)、P2P 通訊、共識機制、分散式儲存及智慧型合約(Chaincode)等技術組合，可以在沒有第三方公正機構情形下，解決雙方或多方交易過程的互不信任問題。其中，共識機制是 BC 的核心元件，任何節點發起交易，會向其他節點廣播資料，收到資料節點先使用數位簽章機制，驗證發起交易的節點，驗證成功後，其他節點就開始執行共識演算，一些眾所周知的共識演算法包括工作量證明(Proof-of-Work)、權益證明(Proof-of-Stake)，而智慧型合約則是一組程式碼，可在交易中觸發執行。

作者使用 BC 作為分散式儲存系統，當資料進入 Broker 節點如圖 48 所示，Broker 1 會發起交易，將資料廣播給其他節點，收到資料的節點會驗證 Broker 1 的數位簽章，同時此交易會觸發智慧型合約去檢查資料，當達成共識，資料才能進入 BC。

3.25 Gowri Sankar Ramachandran, Kwame-Lante Wright, Bhaskar Krishnamachari. (2018). Trinity: A Distributed Publish/Subscribe Broker with Blockchain-based Immutability Retrieved from <https://arxiv.org/pdf/1807.03110.pdf> (Jul. 03, 2023)

3.28 Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding, Aruna Seneviratne. (2020). Blockchain and Edge Computing for Decentralized EMRs Sharing in Federated Healthcare. Retrieved from <https://ieeexplore.ieee.org/document/9347951>

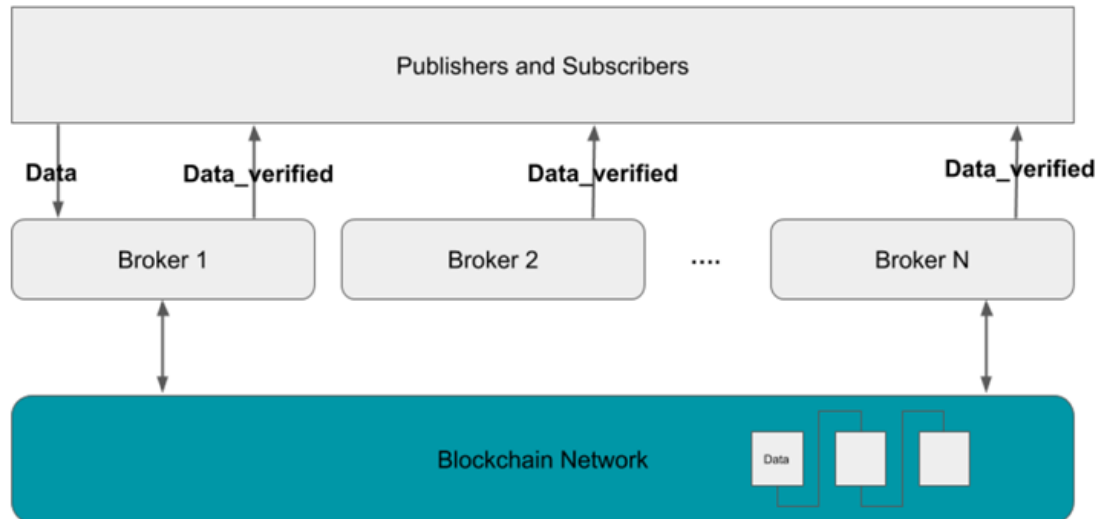


圖 48、分散式儲存系統示意圖

資料來源：請參閱附錄-參考資料^{3.25}

上述的流程達成，除 Broker 1 外所有節點使用數位簽章機制驗證 Broker 1，達成去中心化的認證機制，Broker 1 數位簽章及資料都會記錄在 BC，達成資料不可變性，任何用戶無法篡改資料。認證機制及資料儲存都為分散式，資料不須回傳核心網路，可減少延遲時間，每個 BC 節點保有所有資料的副本，且 BC 節點都有與外界溝通的應用層，可以實作容錯機制。

使用 BC 記錄 IoT 裝置產生的資料，除了資料量太大外，BC 節點廣播資料給所有節點也可能造成網路瓶頸。IEEE^{3.28} 建議結合 IPFS 解決此問題。IPFS 是以分散式系統來儲存資料與分享資料的 P2P 網路傳輸協定，使用內容的摘要值去找資料。IPFS 檔案都儲存在 IPFS 物件中，每個物件最多 256 KB，若檔案大於 256 KB，會被分割為多個物件，再使用分散式傳輸協定傳送到其他節點，因此存取檔案不會

3.25 Gowri Sankar Ramachandran, Kwame-Lante Wright, Bhaskar Krishnamachari. (2018). Trinity: A Distributed Publish/Subscribe Broker with Blockchain-based Immutability Retrieved from <https://arxiv.org/pdf/1807.03110.pdf> (Jul. 03, 2023)

3.28 Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding, Aruna Seneviratne. (2020). Blockchain and Edge Computing for Decentralized EMRs Sharing in Federated Healthcare. Retrieved from <https://ieeexplore.ieee.org/document/9347951>

有單點失敗的問題。但是會有取不到資料的情況，例如檔案分散在 10 個節點上，而這 10 個節點都剛好都失效。此論文並未針對這些問題進行討論，只建議將實際資料存放在 IPFS，BC 僅儲存資料的摘要值。針對讀不到資料的問題，可以用儲存較多的副本緩解，但合理的副本數將於實證計畫中進行探討。

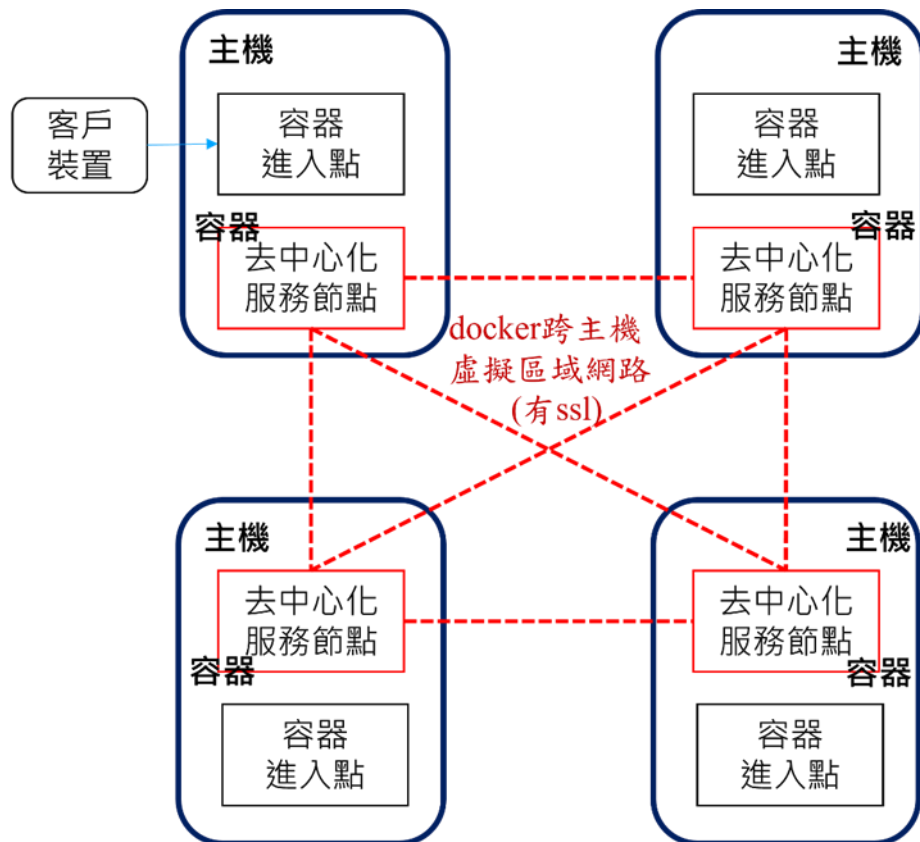
除上述問題，此 2 篇論文也未解決隱私保護問題，因 BC 資料的不變性及透明性，攻擊者可以透過分析公開帳本威脅使用者隱私，因此需要利用 IPFS 鏈下的儲存空間，加入存取控制機制，達成區塊刪除效果的 API。

最後必須探討 BC 節點數與 BC 安全的問題，當節點數太少，惡意參與者可以控制最長鏈的產出，若節點數太多又會影響效能，此問題於實證計畫中進行探討。

二、去中心化管理機制運作

延續前述情境設定，即是組織或公司使用第三方提供商或電信業者所提供的 IoT MEC Gateway，連結企業內部其他裝置與 IoT 邊緣管理平臺。首先，分析 IoT 邊緣管理平臺如何安全連結多個 MEC 上的 BC、IPFS 及 MQTT Broker 節點，目前 5G 開源計畫如 free5GC，皆以容器化虛擬技術建置；或如 Docker，輕量化的容器化虛擬技術就是一個應用程式的行程，由於無須塞入整套作業系統，不僅減少運算資源、RAM 空間與儲存容量的開銷。現在有許多雲端資料中心採用，透過容器進行資源隔離，實現更快速的應用程式生命週期管理，更兼顧虛擬機器的隔離性與快速部署服務的彈性。而這趨勢也逐漸延伸到邊緣，如奇異公司 (GE) Predix 軟體平臺、亞馬遜雲端運算服務 (Amazon Web Services, AWS) IoT 邊緣運算平臺 Greengrass 和 Microsoft Azure IoT Edge 都是透過容器技術，將原本雲端的工作負載移至邊緣。因此透過 BC、IPFS 及 MQTT Broker 節點預計以 Docker

跨主機의 虛擬區域網路連結，並開啟各容器的安全資料傳輸層 (Secure Socket Layer, SSL) 設定確保連線安全，架構如圖 49。



- 去中心化節點以docker虛擬區域網路連結組成去中心化服務
- 客戶裝置使用實體網路連結任一容器進入點，取得服務

圖 49、去中心化管理機制運作

資料來源：本計畫整理

接著討論分散式儲存系統的存取 API，BC 應用層是對外溝通的管道，針對前面設定的情境，需開發資料摘要值存取 API，API 實質上即是執行一個 BC 交易，因此無授權者無法存取資料，以確保零信任最小需求。IPFS extension 開發 IPFS 存取控制，讓特定資料無法讀取，達成類似刪除區塊的效果。IoT Broker 備援機制，當 Broker 節點失效，需透過 BC 應用層 API 取回資料重啟，概略的系統階層如圖 50 所示。



BC應用層 API	IPFS extension	Broker備援 API
BC	IPFS	MQTT Broker
P2P網路		
docker container VLAN with SSL		

圖 50、系統階層圖示意圖

資料來源：本計畫整理

第三節 跨領域應用情境的安全與可靠實證先導評估

一、實證目的

實證計畫使用 DLT 技術建置分散式認證機制及儲存系統，將資料及計算都留在邊緣環境的可行性。雖然國際組織也建議以 DLT 技術來建構新型態的安全架構及分散式儲存系統以達成 6G 關鍵指標，但這樣的趨勢還處於發展初期，許多標準尚未制定完成，已發表的技術文件也須整合測試，因此本計畫將藉由比較中央式的認證機制及儲存系統效能的過程，檢驗何種 DLT 流程適合低延遲的應用。同時也架設分散式 IoT 系統，與中央式 IoT 系統比較，進行容錯能力評估。

二、測試方法

實證計畫選擇將 BC 等分散式系統的節點建立在 MEC 伺服器，是因邊緣運算環境會部署於基地臺旁，如圖 35 所示，當進入 B5G/6G 後，基地臺數量將會急速增加，應有夠多的 MEC 伺服器用於建立叢集節點以組成 BC、IoT 等分散式系統。BC 系統在測試流程將提供分散式認證功能，實證計畫假設使用者會向 BC 系統註冊，註冊程會產出：

(一)使用者錢包(Wallet)，錢包存放有公開金鑰 (Public Key)、私密金鑰(Private Key)及去中心化身分 (Decentralized Identity, DID)。

(二)使用者 Public Key 會經由圖 39 的 Building New Block 步驟，在 BC 節點間達成共識寫入 BC，其他用戶可由 DID 取得 Public Key。

在此假設下，使用者要取得服務只要送出 DID 及簽章給服務商要求服務，收到訊息的服務商由 BC 取得 Public Key，就可完成驗證使用者，流程示意圖如圖 51，除非有其他交易，才需進行圖 39 完整的交易流程。

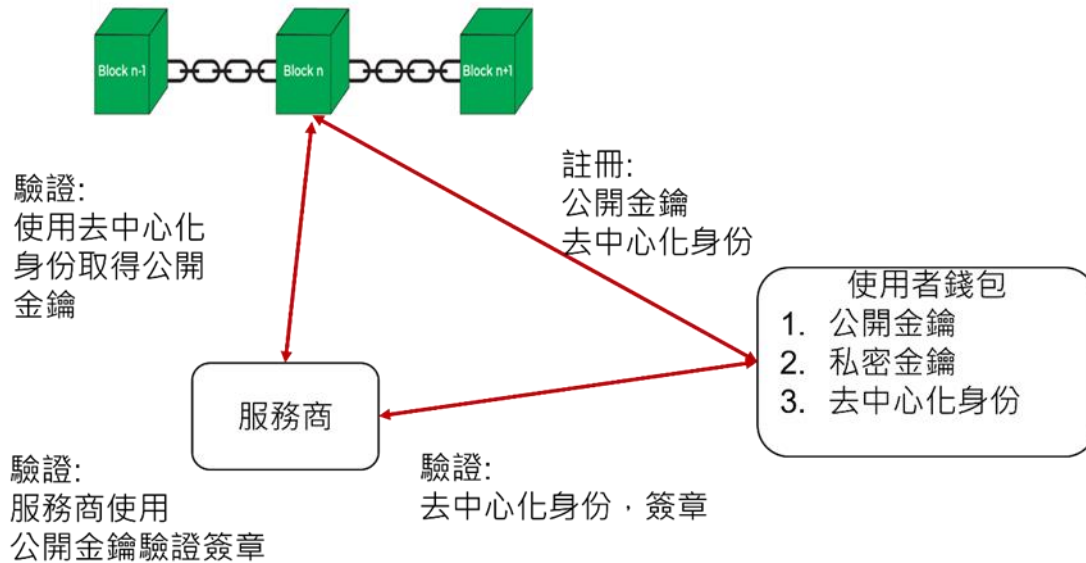


圖 51、BC 驗證流程示意圖

資料來源：本計畫整理

(一)分別在邊緣運算環境及 Google 雲端虛擬主機安裝 RADIUS 認證伺服器，比較分析圖 51 的認證機制效能，評估排除在雲端部署中央式認證機制的可行性。

(二)測試以網路元件監看機制所實作的容錯機制，先建立虛擬網路元件監看機制，再模擬元件失敗，記錄系統再次產生元件的時間。

(三)分散式儲存系統測試，在邊緣運算環境結合 IPFS 及 BC 架設分散式儲存系統，記錄讀取與寫入的時間，並模擬節點失敗，記錄系統提供服務的狀態。

三、測試環境及架構

由於 6G 電信網路將走向電信基礎建設分享及多租戶等新型商業模式，虛擬化技術是必要的基礎技術，因此應用雛型系統預計選擇容器化的開源計畫為基礎環境，如圖 52 中 5G 核心站點(5G Core Site)及 MEC 平臺(MEC Platform)會選取以 Docker 為基礎的開源計畫，再向上建構去中心化認證架構及儲存系統。

測試環境架構會以 Docker 容器技術部署如圖 52，5G 核心站點由多個核心網路容器組成以提供核心網路功能，實證測試環境主要使用 5G 核心站點的 UPF 容器將無線電存取網路訊息(Radio Access Network message, RAN message)傳遞到 MEC 平臺，用於模擬基地臺分流的功能。MEC 平臺也是使用 Docker 容器建置，BC 節點及 IPFS 節點分別表示 BC 節點及分散式儲存系統 IPFS 節點，一個 MEC 平臺只會包含少數節點，需要多個 MEC 平臺才能組成 BC 及 IPFS 系統，其中 BC 系統會提供認證功能，並與 IPFS 結合模擬邊緣環境的分散式儲存系統。MEC 平臺中 Broker 節點是 IoT 系統的代理者節點，同樣需要多個節點才能模擬分散式 IoT 應用情境。

前述所有網路功能都是以 Docker 容器技術產生，各容器的連結則由 Docker 虛擬網路技術設定，這即是網路功能虛擬化基礎設施(Network Functions Virtualization Infrastructure, NFVI)所提供的功能。

實證計畫會以多個 MEC 平臺建構 BC 服務、分散式儲存系統及 IoT 應用服務，測試分散式系統在邊緣環境的可行性及效能。

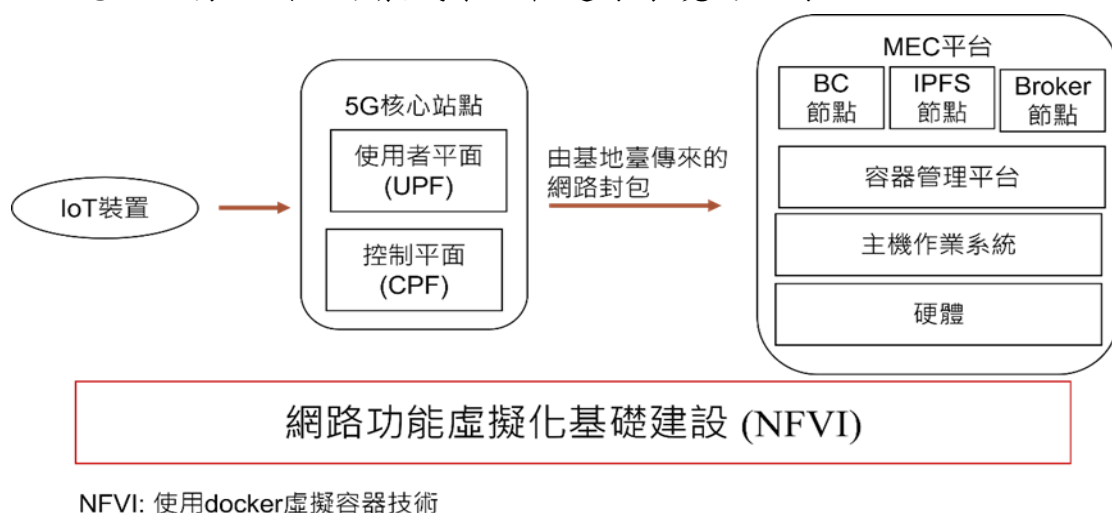


圖 52、基礎環境示意圖

資料來源：請參閱附錄-參考資料^{3.29}

3.29 Cloud RAN and MEC: A Perfect Pairing (2018) Retrieved from https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp23_MEC_and_CRAN_ed1_FINAL.pdf

本實證測試系統架構底層為實體主機，再以虛擬軟體建置至少 3 個虛擬主機，分別以 NFVI 在 3 個虛擬主機上建置 IoT 裝置、5G 核心站點及 MEC 平臺所需之 Docker 容器。容器集包含 5G 核心站點程式集、UE 模擬程式及 MEC 平臺程式集的執行程序及資料，目前系統是一個程式在一個容器中執行，如圖 53 所示。

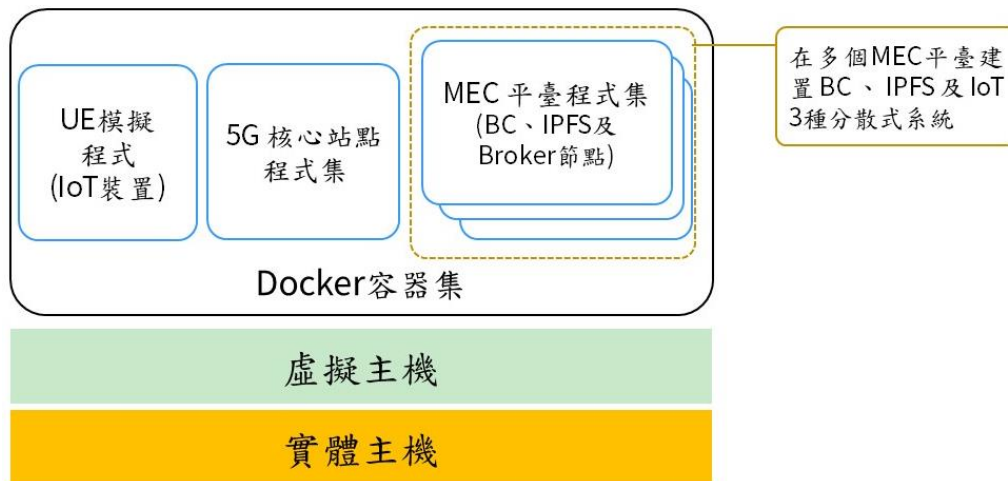


圖 53、跨領域應用情境的安全與可靠實證測試系統架構圖

資料來源：本計畫整理

四、使用之軟硬體

實證測試環境使用虛擬主機，安裝虛擬主機的 Linux 實體主機規格如表 22 所示：

表 22、實體主機規格

名稱	裸機
硬體規格	- 中央處理器 AMD Ryzen 9 2.2GHz 12 Cores - 記憶體 128 GB RAM 及 2 TB 硬碟
作業系統	Ubuntu 20.04
程式軟體	虛擬軟體 VirtualBox 7.0
網路介面	802.3
備註	一個裸機預計安裝 6 個虛擬機器，平均每個節點會使用 2 個虛擬機器，將安裝 MEC 節點、Core 節點及 UE 節點

資料來源：本計畫整理



實體主機將安裝多個虛擬主機，並將 5G 核心站點及 MEC 平臺安裝於虛擬主機。虛擬主機規格如表 23 及表 24 所示：

表 23、5G 核心站點虛擬主機規格

名稱	核心網路節點
硬體規格	虛擬機器規格： • 2 Cores • 8GB RAM • 100 GB 硬碟
作業系統	Ubuntu 20.04
程式軟體	• 容器管理工具為 Docker 24.0.6 • 安裝的軟體 free5gc-v3.1.1
網路介面	802.3 容器網路介面
備註	使用 2 臺虛擬機器組成 1 個 Core 節點，每個虛擬機器的硬體規格皆為 2 Cores、8GB RAM 及 100 GB 硬碟

資料來源：本計畫整理

表 24、MEC 平臺虛擬機器規格

名稱	MEC 節點
硬體規格	虛擬機器規格： • 2 Cores • 8GB RAM • 100 GB 硬碟
作業系統	Ubuntu 20.04
程式軟體	• 容器管理工具為 Docker 24.0.6 • 安裝的軟體：free5gc-v3 的 UPF、BC 系統 VON Network、分散式系統 IPFS 及 IoT 系統 vernemq
網路介面	802.3 容器網路介面
備註	使用 2 臺虛擬機器組成 1 個 MEC 節點，每個虛擬機器的硬體規格皆為 2 Cores、8GB RAM 及 100 GB 硬碟

資料來源：本計畫整理



除了 5G 核心站點及 MEC 平臺之外，還需安裝 UE 模擬器，虛擬機器規格如表 25 所示：

表 25、UE 虛擬機器規格

名稱	UE 節點
硬體規格	虛擬機器規格： • 4 Cores • 8GB RAM • 50 GB 硬碟
作業系統	Ubuntu 20.04
程式軟體	• 容器管理工具為 Docker 24.0.6 • 安裝的軟體有 free5gc-v3 • 行動裝置模擬器為 UERANSIM
網路介面	802.3 容器網路介面
備註	使用一臺虛擬機器組成 1 個 UE 節點

資料來源：本計畫整理

五、測試步驟

實證計畫實施 3 種測試，測試步驟如表 26 至表 28 所示。

表 26、測試 1-評估分散式管理機制

測試項目	測試評估以容器技術建置分散式管理機制之效能及延遲時間
測試步驟	1. 分別在邊緣運算環境及 Google 虛擬機器執行 RADIUS 伺服器。 2. 在 UERANSIM 模擬環境執行 RADIUS 客戶端程式與 RADIUS 進行認證流程，並記錄時間。 3. 在 UERANSIM 模擬環境執行圖 51 的驗證/註冊流程，並記錄時間。

資料來源：本計畫整理

表 27、測試 2-評估容器監看回復機制

測試項目	評估容器監看回復機制，對 MQTT 代理者接收訊息的影響
測試步驟	1. 在邊緣運算環境置使用 venermq 開源方案架設 MQTT 代理者群集，再用 MQTT UE 端模擬器傳遞大量訊息。 2. 將代理者停止在回復，觀察 MQTT 代理者群訊息丟失的情形。

資料來源：本計畫整理

表 28、測試 3-評估分散式儲存系統

測試項目	評估分散式儲存系統的讀取及寫入時間
測試步驟	1. 在邊緣運算環境建置 IPFS 系統，再整合 BC 架設分散式儲存系統。 2. 記錄分散式儲存系統的存取資料時間。 3. 將分散式儲存系統的節點停止，記錄回復服務時間。

資料來源：本計畫整理

六、測試數據及測試結果之探討

(一)測試 1—評估分散式管理機制

比較集中式認證機制與 BC 所提供的分散式認證機制之延遲時間，其中集中式認證機制為 RADIUS 認證協定。為此，本計畫設想 4 種情境，如圖 54，測試情境說明如下：

1. 情境 A：RADIUS 伺服器安裝在 Google 虛擬機器上，RADIUS 客戶端程式則執行在 UERANSIM 模擬器上，使用 free5gc 提供的網路介面，進行 EAP-TLS 認證程序。
2. 情境 B：UERANSIM 模擬器上，執行圖 51 的驗證流程，驗證流程為使用者使用送出 DID 及數位簽章給服務商要求服務，收到要求的服務商由 BC 取得 Public Key，完成驗證使用者程序。

3. 情境 C：RADIUS 伺服器在邊緣運算環境的機器上，RADIUS 客戶端則執行在 UERANSIM 模擬器上，使用 free5gc 提供的網路介面，進行 EAP-TLS 認證程序。
4. 情境 D：UERANSIM 模擬器上，執行圖 51 的註冊及驗證流程，與情境 B 的差異為使用者使用送出服務要求前，將個人 Public Key 透過 BC 程式介面寫入 BC，在進行驗證。

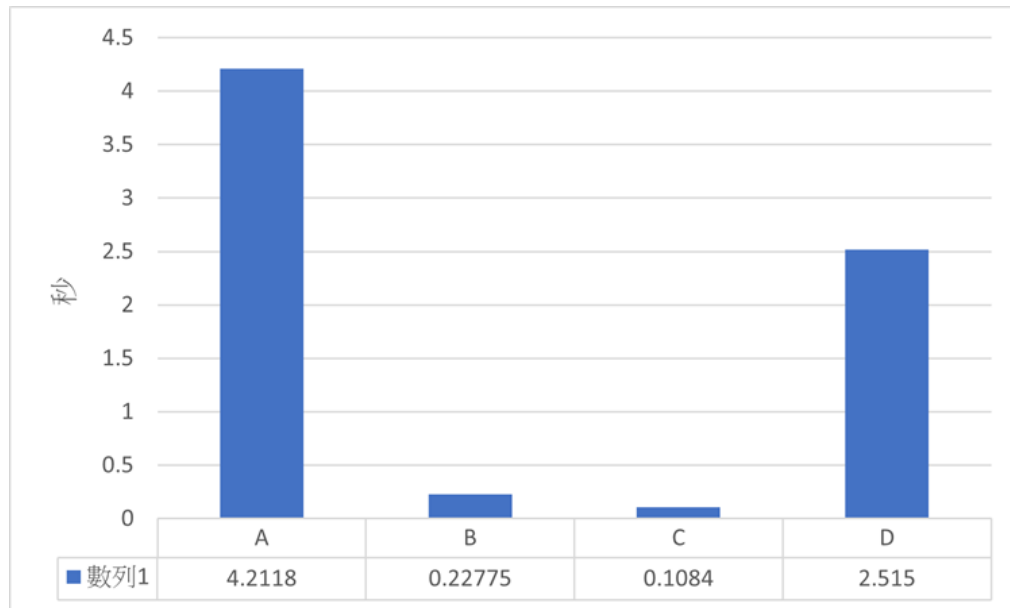


圖 54、認證延遲時間比較圖

資料來源：本計畫整理

本實證 4 種情境測試結果分別為圖 54 之 A、B、C、D 標記，根據測試結果進行比較分析與探討，分別說明如下：

1. 情境 A 與情境 C 比較：情境 A 與情境 C 都是針對 RADIUS EAP-TLS 認證程序做測量，主要差異為 RADIUS 伺服器的安裝位置，情境 A 花費最多回合認證訊息傳遞，其餘的計算時間跟情境 C 相差不大，如圖 55，計算時間為紅線以下，記錄時間為 10 次實驗中的節錄，情境 A 與情境 C 的密碼演算法皆為 RSA2048 位元及 SHA256，因此計算時間差不多，主要差異為訊息傳遞時間。

real	0m4.489s	real	0m0.108s	完成流程 的時間
user	0m0.021s	user	0m0.021s	計算時間 (Sha256 , RSA 2048)
sys	0m0.013s	sys	0m0.028s	
情境 A		情境 C		

圖 55、情境 A 與情境 C 比較圖

資料來源：本計畫整理

2. 情境 B 與情境 C 比較：情境 B 執行圖 51 的驗證流程，BC 系統安裝於邊緣環境，使用的密碼演算法為 Sha256，橢圓曲線的演算法 256 位元，與情境 C 的差異為計算時間。
3. 情境 B 與情境 D 比較：情境 B 與情境 D 的執行環境一致，同樣使用 Sha256 及橢圓曲線的演算法 256 位元，使用 BC 系統也安裝於邊緣環境。主要差異為圖 51 的註冊流程，註冊流程需要 BC 系統共識流程，因此增加許多計算時間，且會隨節點增加而增加，因為要有超過一半的節點數達成共識才能將資料寫入 BC，如圖 56，在 4 個節點的 BC 系統須至少 3 個節點達成共識。

```
{ 'multi_signature': { 'participants': [ 'Node2',
                                         'Node3',
                                         'Node1'],
  'signature': 'QpYF0SRrAr2orHf' }
```

圖 56、情境 B 與情境 D 比較-節點共識示意圖

資料來源：本計畫整理

實驗結果顯示中央式的認證機制會讓邊緣環境無法完全達成預期的效果，主要是認證流程所需回合數較多，造成傳遞延遲，而以邊緣環境的 BC 系統來設計認證機制，將有機會降低延遲，若能避免使用需要共識機制的 BC 系統程式介面，則可大幅降低延遲時

間。除此之外，測試 1 也在測試認證的過程，以重啟容器方式模擬節點失效，重啟的過程 BC 系統會轉換到其他節點，而 RADIUS 則會等到重啟完成，因此產生的延遲時間較多，如圖 57，這樣的結果顯示 BC 系統可以緩和單點失效，同時 BC 系統的分散式帳本可作為電信業者帳務審計的基礎。

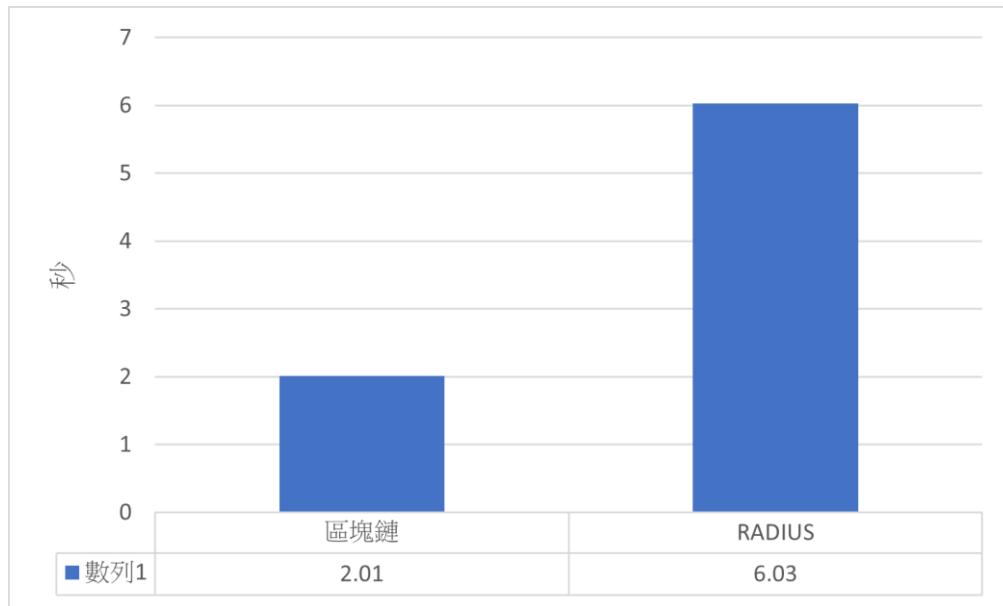


圖 57、包含重啟的認證延遲時間

資料來源：本計畫整理

(二)測試 2—評估容器監看回復機制

MQTT 代理者都以 Docker 容器建立，數個代理者容器以虛擬網路連結成群集並且分散於不同實體主機，群集中的數個代理者可依據指定的協定埠 (Protocol port) 共同分擔不同來源的訊息以達成負載平衡。依此特性，測試 2 使用 2 個協定埠，將群集區分成 2 組，其中一組只包含單一代理者，另一組則包含剩下代理者，再以 MQTT 模擬器模擬 100 個客戶端透過代理者群集訂閱 100 次訊息，進行訊息處理吞吐量及回復機制測試，其中訊息處理吞吐量為代理者群集每秒處理的訊息總數。圖 58 表示不同大小的代理者群集的訊息處理吞吐量回隨著代理者數量增加而變大。除此之外，MQTT

模擬器隨機使用代理者所在主機的 IP 位址(IP Address)發送訊息，都可以完成模擬程序，這也隱含表示以容器技術架設的代理者群集可以緩和單點失效的問題。

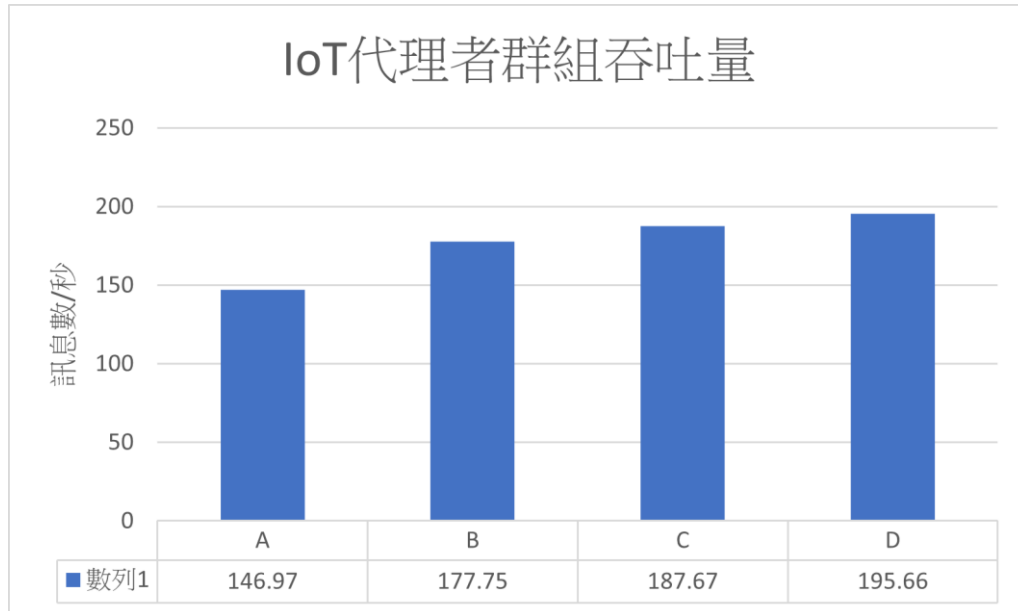


圖 58、IoT 代理者群組吞吐量

資料來源：本計畫整理

將容器故意停止後回復，MQTT 代理者群集沒有資料丟失的情形，這可能是因為容器回復時間很快，但若將虛擬機器關機，則資料丟失情形便提升，這是因為群集的其他代理者無法判斷是停止還是離開，只有代理者離開群集其他代理者才會介入，否則要靠自己回復，以避免訊息序列被破壞。

(三)測試 3—評估分散式儲存系統

結合 IPFS 與 BC 所組成的分散式儲存系統的寫入及讀取時間如圖 59 所示，寫入的時間明顯大於讀取時間，這是因為系統的存取流程都使用 BC 程式介面，寫入儲存系統相當於建立新區塊，需要進行 BC 節點間的共識流程，且時間會因節點數增加而增加，因此不適合當成資料庫使用。但 BC 提供不同參與者建立信任的機制與審計能力，可用於發展跨不同公司或組織的資料分享平臺。

在節點回復的測試中，發現容器回復時間與容器中的伺服器回復時間接近，這是因為容器本身也是主機上的一個行程，許多原本的系統回復狀態都記錄容器平臺，使得回復速度較真實主機快。

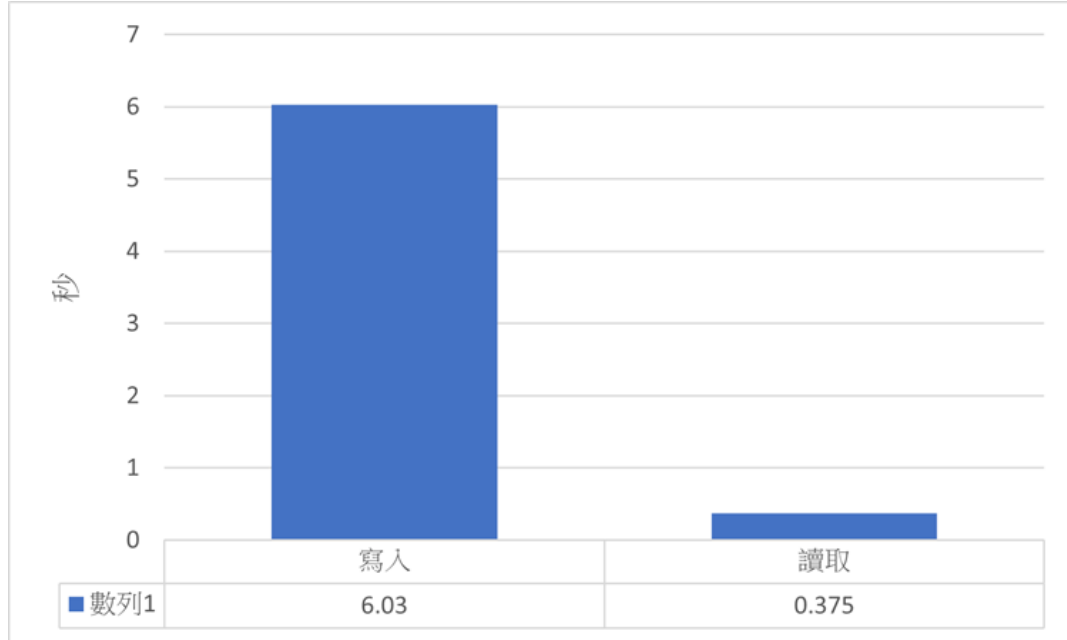


圖 59、分散式系統存取時間

資料來源：本計畫整理

第四節 小結

本計畫中研析各種虛擬技術，包括 NFV、SDN 以及 NFV 編排器，同時探討各種虛擬技術如何在實體網路上架構虛擬網路。目前各國國際組織是以 DLT 技術建置 BC 系統對應新型態的安全框架之需求，標準制定狀態如下：

一、ETSI—聯合資料管理技術

引入 DLT 技術初期，ETSI 先就 DLT 基本技術說明，這些基本技術包括 BC 架構、智慧合約及共識流程，如標準^{3.30、3.31}說明如何建置/使用 BC，同時在另一份標準^{3.21}建議核心網路須連上 BC，如圖 41 所示，以及不同 BC 的互通說明。在 DLT 定義完備後，ETSI 開始結合邊緣運算技術及 IoT 技術，討論如何使用 DLT 技術在邊緣運算如何管理資料^{3.21}，管理的動作包括收集、儲存、分享及計算，在另一份群組報告^{3.18}，更提到使用 FL 將大量 IoT 裝置產生的資料轉換成 AI 模型，以模型取代資料減少傳輸量，同時緩和資料隱私問題。這樣的技術演進符合邊緣智慧的發展趨勢，也就是讓資料就近在邊緣環境處理。

二、ITU—IOT 及智慧城市應用

如同 ETSI，ITU 也針對 DLT 基本技術進行探討，但 ITU 則更進一步針對系統架構及下一代電信網路應用情境進行討論，在 Y.2342^{3.32}

3.30 ETSI GR. (2020). Permissioned Distributed Ledger (PDL); Application Scenarios Retrieved from https://www.etsi.org/deliver/etsi_gr/PDL/001_099/003/01.01.01_60/gr_PDL003v010101p.pdf

3.31 ETSI GR. (2021) Permissioned Distributed Ledgers (PDL) Smart Contracts System Architecture and Functional Specification. Retrieved from https://www.etsi.org/deliver/etsi_gr/PDL/001_099/004/01.01.01_60/gr_PDL004v010101p.pdf

3.21 Draft ETSI GS PDL 013 V0.0.1 (2021-12); Permissioned Distributed Ledger (PDL); PDL for Supporting Distributed Data Management (Draft)

3.18 ETSI GR PDL 009 V1.1.1 (2021-09) Permissioned Distributed Ledger (PDL); Federated Data Management.

https://www.etsi.org/deliver/etsi_gr/PDL/001_099/009/01.01.01_60/gr_PDL009v010101p.pdf

3.32 ITU_Y.2342. (2019). Scenarios and capability requirements of blockchain in next generation network evolution Retrieved from <https://www.itu.int/rec/T-REC-Y.2342/en>

討論國際漫遊及資料分享等情境，在 Y.3530^{3.20} 標準說明 BC 即服務的系統架構，同時也說明不同 BC 系統如何互通，如圖 40 所示。

在 BC 技術定義完備後，ITU 的討論群組 SG20，則使用 BC 技術定義 IoT 相關標準，如 ITU-T Y.4464^{3.27} 定義使用 BC 為存放 IoT 應用資料的分散式儲存系統，而標準 ITU-T Y.4486^{3.17} 則更進一步針對 IoT 裝置部署於邊緣環境進行討論，同時探討使用 DLT 技術存取部署於邊緣環境的去中心化服務，例如加速車載 IoT 分享道路即時資訊。除此之外 ITU-T^{3.33} 也提及 ITU-T Series F 將進行 AI 與 DLT 技術結合的探討，但目前只有概念性說明。

三、其他組織—DLT 基本技術探討

目前其他國際組織大都還在探討 DLT 基本技術，就目前收集到的資訊來看，只有 IEEE 2144.1-2020^{3.22} 聚焦在 IoT 資料處理與 ITU-T Y.4464^{3.27} 類似。

就資料管理觀點，ETSI 以分散式資料管理^{3.21} 及聯合資料管理^{3.18} 2 個技術項目探討如何管理邊緣運算環境所產生資料，其中又以 IoT 系統產生的資料為重點。2 項技術的主要原則就是資料就近在邊緣運算環境處理，並建議使用 DLT 技術處理資料，其中處理的程序包括資料如何被發現、儲存及計算，其中計算則建議使用 FL 及多方計算

3.20 ITU-T Y.3530. (2020). Cloud computing - Functional requirements for blockchain as a service Retrieved from <https://www.itu.int/rec/T-REC-Y.3530/en>

3.27 ITU-T Y.4464. (2020). Framework of blockchain of things as decentralized service platform. Retrieved from <https://www.itu.int/rec/T-REC-Y.4464>

3.17 ITU-T Y.4486. (2023) Framework of cross edge decentralized service by using DLT and edge computing technologies for IoT devices. Retrieved from <https://www.itu.int/rec/T-REC-Y.4486>

3.33 ITU-T. Series F. (2021) SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES Overview of convergence of artificial intelligence and blockchain

3.22 IEEE (2020) Standard for Functional Requirements in Blockchain-based Internet of Things (IoT) Data Management. Retrieved from https://standards.ieee.org/standard/2144_1-2020.html.

3.21 Draft ETSI GS PDL 013 V0.0.1 (2021-12); Permissioned Distributed Ledger (PDL); PDL for Supporting Distributed Data Management (Draft)

3.18 ETSI GR PDL 009 V1.1.1 (2021-09) Permissioned Distributed Ledger (PDL); Federated Data Management.

https://www.etsi.org/deliver/etsi_gr/PDL/001_099/009/01.01.01_60/gr_PDL009v010101p.pdf

(Multi-Party Computation) 以避免大量原始資料在網路傳遞而降低邊緣運算環境效能，關於此點，ITU_Y.4486^{3.17} 進一步建議將大量的 IoT 裝置分成許多小群，數個小群由一個 BC 系統就近處理身分驗證及資料存取，避免系統過大而降低整體效能。

再以 IoT 應用面出發，部署於邊緣運算環境的大量 IoT 裝置會在不同位置產生資料，這些資料會留在邊緣運算環境處理，將結果儲存於 BC 系統或傳回雲端，就 ETSI 及 ITU 相關文獻看，未來的技術發展會著重於如何藉由 BC 系統分享資料，原因除了要提升系統整體效能以符合 6G 關鍵指標，另一個重點應該是 BC 系統具有公開、公平的審計能力，分享的資料不會被特定組織獨占，這對未來發展智慧城市相關應用是相當重要。

除此之外，各國國際組織都針對 DLT 技術進行討論，討論的範圍不限於金融應用而是擴大到解決集中化架構的信任問題，許多資料被特定組織收集後，資料就變成組織的私產，這對活絡第三方發展應用系統是一大阻力，尤其在智慧邊緣概念成形後，具有公開、公平的資料分享機制將更為重要。

上述的技術演進與智慧邊緣的發展趨勢一致，同時說明邊緣運算環境的節點應該會支援分散式的協作運算，這些協作運算包括 FL、分散式機器學習、多方計算等分散式的計算系統，但不應存在中央式的聚合程序在分散式的計算系統，而上述文件並沒有全面探討。另外，就 ITU_Y.4486^{3.17} 建議將大量的 IoT 裝置分成許多小群，再以 BC 系統進行管理，但也未就群的大小進行與系統效能探討，同時 BC 系統

3.17 ITU_Y.4486. (2023) Framework of cross edge decentralized service by using DLT and edge computing technologies for IoT devices. Retrieved from <https://www.itu.int/rec/T-REC-Y.4486>

的擁有者可能分別屬於不同服務商，這就需要考慮不同 BC 系統互通，雖然多份標準^{3.18、3.20}提及，但目前都只是概念說明。

就目前收集的文獻看來，大量 IoT 裝置將會被分成多個群組，數個群組由部署於邊緣運算環境的 BC 系統管理，雖然在文獻中，BC 系統的擁有者並沒有明確定義，因 IoT 應用面非常廣泛，BC 系統擁有者屬於不同服務商的可能性很高，這將使得實證計畫自行架設私有 BC 系統的經驗以及評估效能經驗有助於服務商建立自己的 BC 系統及評估群組大小與系統效能的關係，但在 BC 系統互通性方面，如何讓服務商間有共同信任基準需要進一步研究，而研究方向應該是建立所有服務商及用戶可信任的 DLT 聯盟。若是在邊緣運算環境建立可以被廣泛信任的 DLT 聯盟，實證計畫情境 C，以 DLT 身分驗證取代雲端 RADIUS 認證的概念，推廣到取代單一簽入(Single Sign-On)服務，因為現行單一簽入程序同樣需要在客戶端與雲端之間進行多回合訊息傳送，會產生較多的延遲，因此部署於邊緣運算環境的去中心化服務應該避免使用，才可以完全發揮邊緣運算環境的優勢，而實證計畫情境 C 的概念可以做為參考。

3.18 ETSI GR PDL 009 V1.1.1 (2021-09) Permissioned Distributed Ledger (PDL); Federated Data Management.

https://www.etsi.org/deliver/etsi_gr/PDL/001_099/009/01.01.01_60/gr_PDL009v010101p.pdf

3.20 ITU_Y.3530. (2020). Cloud computing - Functional requirements for blockchain as a service Retrieved from <https://www.itu.int/rec/T-REC-Y.3530/en>

第四章 建立 6G 應用自動攻防與情資離型系統先導評估

本工作項目研析 6G 與 5G 在網路威脅方面的差異，以利釐清 6G 資安需求，接著研析 5G 環境下的滲透測試規範，包含國外對於 5G 核網的滲透測試以及台灣資通產業標準協會(Taiwan Association of Information and Communication Standards, TAICS)所制定的 5G IoT 場域滲透測試規範，這些資訊將可做為未來 6G 環境下，對通訊網路與 IoT 應用擬定滲透測試規範的參考依據。資安威脅無處不在，從現有 5G 環境所發動的傳統網路攻擊，例如：IP Spoofing、DoS、Downgrade Attack 等進行分析研究，可以瞭解其攻擊的手段、特徵、造成的影響及緩解的方式，並且有助於探索新技術發展，例如：AI 或新的通訊技術於未來 6G 通訊設備或服務的實際應用上，可能遭受的攻擊與潛在的影響。因此，針對網路攻擊下 AI-Native Security、in-X 子網 Network Slicing Security 等非傳統資安威脅進行研究分析，包含可能攻擊手法、防禦或緩解措施及影響、偵防工具化的可行性等，將有助於提早布局與發展未來 6G 時代的資安防護技術。本章同時介紹國家資安資訊分享與分析中心(National Information Sharing and Analysis Center, N-ISAC)之 STIX 的研析成果。期望藉由本工作項目之研析，找出目前 N-ISAC 之情資格式之不足，並提供可能的解決方法，以提升政府情資分享架構在 6G 環境之可用性。

在實證先導評估的部分，模擬 6G 網路引入 AI 模型做無線網路資源智慧化配置，以及該 AI 模型遭受 DoS 攻擊、對抗性攻擊的衝擊評估。觀測 RAN 遭受攻擊的結果，以及啟動防禦機制的成效，同時將收集與分析 UE 端量測數據。

第一節 建立 6G 應用自動攻防與情資離型系統說明

一、6G 與 5G 在網路威脅方面的差異

在評估 6G 資安需求之前，先從 6G 預期的特性，來觀察 6G 與 5G 在網路威脅方面的差異如圖 60，將依規模和複雜性、邊緣運算與網路切片、AI 與 ML、隱私與資料保護等 4 個面向進行差異說明：

6G與5G在網路威脅方面的差異



圖 60、5G 與 6G 在網路威脅的差異

資料來源：請參閱附錄-參考資料^{4.1}

(一)規模和複雜性

6G 網路比 5G 具更大規模和更高的複雜性，6G 網路連接的裝置數量將遠超 5G，且將引入更高級的網路技術和服務。然而，這也使得 6G 網路對於潛在網路威脅更為敏感，需要更多的安全機制來保護網路和用戶。

4.1 Abdel Hakeem SA, Hussein HH, Kim H. Security Requirements and Challenges of 6G Technologies and Applications. Sensors (Basel). 2022 Mar 2;22(5):1969. doi: 10.3390/s22051969. PMID: 35271113; PMCID: PMC8914636.

(二)邊緣運算與網路切片

在 6G 時代，邊緣運算與網路切片的技術將更加成熟，能夠提供更高效、更個性化的服務。然而，這種分散式架構可能會導致更多的安全漏洞，需要在每個網路層級都考慮到安全防護。

(三)AI 與 ML

6G 將會利用更先進的 AI 和 ML 技術來優化網路性能及服務。然而，這些技術可能也會被攻擊者利用來發動更複雜、更難以防範的網路攻擊。

(四)隱私與資料保護

6G 處理的資料量比 5G 多，包括個人和敏感資料。因此，在保護用戶隱私和資料安全的同時，利用這些資料來提供高品質服務，將是 6G 面臨的重大挑戰。

二、6G 資安需求說明

前一小節 4 個面向說明未來 6G 時代相較於 5G 所帶來的新形態網路威脅如圖 61，本計畫將探討 6G 資安的需求。由於 6G 預計大大增加裝置間的連接性和資料傳輸速度，將需要一種全新的架構來確保網路的穩定性和可靠性，同時也能處理大量的資料流量。此外，6G 將延續 5G 低延遲特性，會將其提升到一個新層次，因此需要即時高效的網路管理和調度機制，以保證網路性能。在未來的應用面上，6G 將支援更豐富的使用情境，包括虛擬實境、增強實境、自動駕駛和智慧城市等，對於網路頻寬和可靠性的需求將大幅提升。因此 6G 需要能夠滿足高資源需求應用的網路架構。在進入 6G 時代時，IoT 的應用預期將更為廣泛，代表有更多裝置需要連接到網路，並且這些裝置可能位於硬體資源或電力供應有限的環境中，因此 6G 需要具備能在這些條件下提供安全連接的能力。

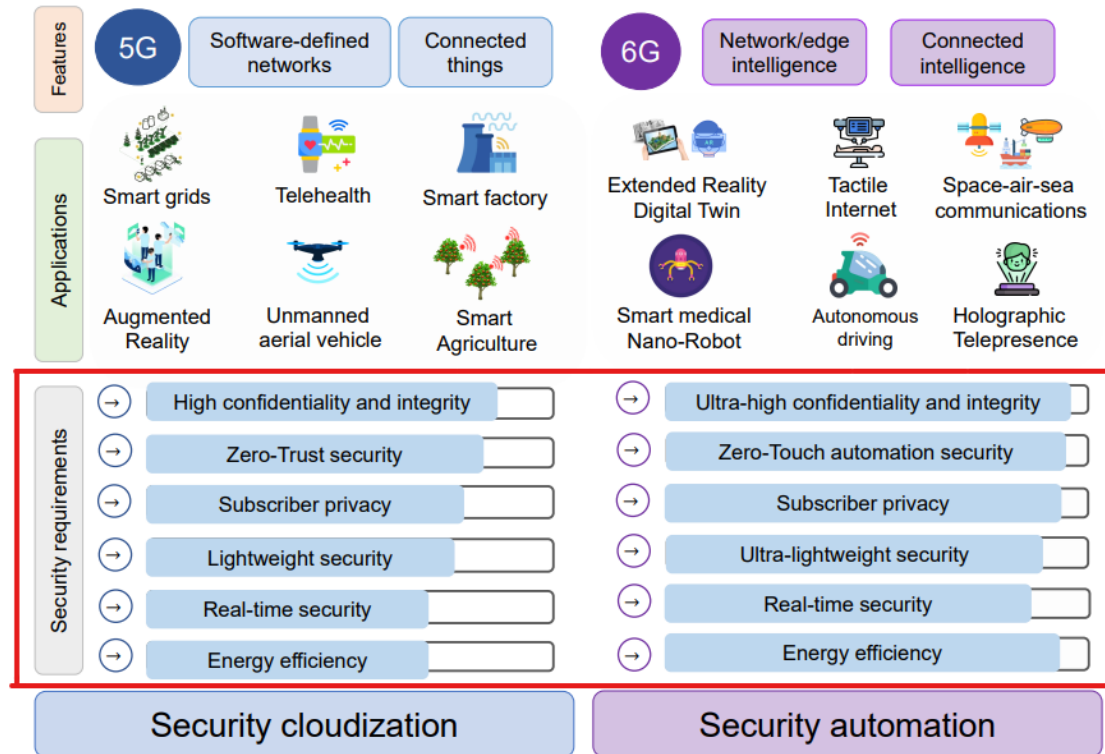


圖 61、從網路特性與應用面比較 5G 與 6G 的資安需求

資料來源：請參閱附錄-參考資料^{4.2}

(一)機密性與完整性 (Confidentiality and Integrity)

隨著進入 6G 時代，由於連接的裝置更加智慧化，將處理大量個人和敏感資料，因此需要更高的安全等級來確保資料之機密性和完整性。無論在傳輸還是儲存過程中，都需要確保資料不被未經授權者存取或更改。持續發展演進的技術包含同態加密 (Homomorphic Encryption)、零知識證明 (Zero-Knowledge Proofs)、安全多邊運算 (Secure Multi-Party Computation)、量子金鑰分發 (Quantum Key Distribution)、DLT 等。

(二)設定自動化 (Zero-Touch Automation Security)

6G 網路將會非常複雜，包含無數的邊緣裝置和智慧化聯網裝置。在此環境下，手動設定和管理網路的安全將變得越來越困難，

4.2 V. -L. Nguyen, P. -C. Lin, B. -C. Cheng, R. -H. Hwang and Y. -D. Lin, "Security and Privacy for 6G : A Survey on Prospective Technologies and Challenges," in IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2384-2428, Fourthquarter 2021, doi: 10.1109/COMST.2021.3108618.

因此需要透過自動化的工具和技術，達成零接觸自動化安全，來確保所有裝置都符合安全標準。

(三)用戶隱私 (Subscriber Privacy)

未來 6G 網路，隱私保護將變得越來越重要。無密碼身分驗證將日漸普及，包含人臉辨識、指紋辨識、虹膜辨識等都有可能應用在用戶身分辨識上。由於 6G 將涉及到更多個人和敏感資料，確保資料在收集、傳輸和儲存過程中的用戶隱私得到有效保護至關重要。

(四)輕量化 (Ultra-lightweight Security)

隨著 6G 網路在邊緣端的應用日益廣泛，考慮到裝置的硬體限制，例如處理能力和電池壽命。因此，需要尋找輕量化的安全解決方案，能在不影響裝置性能之下，提供足夠的安全保護。

(五)即時性 (Realtime Security)

在 6G 網路中，將看到更高的資料傳輸速度和低延遲，將導致任何安全攻擊可能在極短的時間內對網路和連接裝置造成嚴重影響。即時性將變得至關重要，需要能在短暫時間內檢測出潛在的威脅，並立即採取行動來防止或減輕攻擊的影響。這可能涉及到先進的 ML 和 AI 技術，用於即時網路流量分析，在瞬間識別和回應潛在威脅。

(六)能源效率 (Energy Efficiency)

由於 6G 網路將涉及大量的邊緣裝置，包括各種 IoT 設備，這些設備能源效率將是一個重要的問題。如果資安解決方案需要大量的運算資源或網路頻寬，可能會消耗大量的能源，這對於電池供電裝置來說是不可接受的。需要尋找能源效率高的資安解決方案，這可能涉及到加密和認證機制，在提供足夠安全性的同時，也能在能源使用上保持效率。此外，需要考慮如何更智慧化管理和調度網路資源，以降低不必要的能源消耗。

第二節 滲透測試規範蒐集研析

在 6G 環境進行滲透測試是為確保 6G 通訊系統保持高效能，同時具有高安全性，可找出潛在安全漏洞，評估可能遭遇各種威脅的風險等級並修復漏洞。隨著 IoT、邊緣運算和 5G 與未來 6G 技術發展，資通訊安全、資料完整性和個人隱私變得至關重要，滲透測試的執行將可確保未來 6G 網路基礎設施受到惡意活動的影響降到最低，提升 6G 基礎設施安全性並增強客戶信心。

一、5G 核網滲透測試

在 6G 相關標準仍在制定的情況下，先從 5G 環境的滲透測試進行說明，以此做為未來 6G 時代滲透測試的參考做法。在 NIST 所發布的文件^{4.3}介紹 5G 核網參考測試架構如圖 62，包含核網的各功能單元，該單元使用的廠牌，以及測試工具在架構裡測試點的安排，並標示出該測試工具的廠牌。圖 62 中顯示的網路測試節點允許對融合的無線和有線基礎設施、服務和安全功能進行端到端的驗證。例如，可以通過數據、影片或語音的同時連接來壓力測試基礎設施，並觀察模擬用戶的連接速率和吞吐量。一個測試節點可以傳送不同類型的流量：合法的、分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)和惡意軟體。它可以模擬真實世界的應用協議，並允許自定義和操作原始數據。

4.3 NIST. (2022) NIST SPECIAL PUBLICATION 5G Cybersecurity. Retrieved from <https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf>

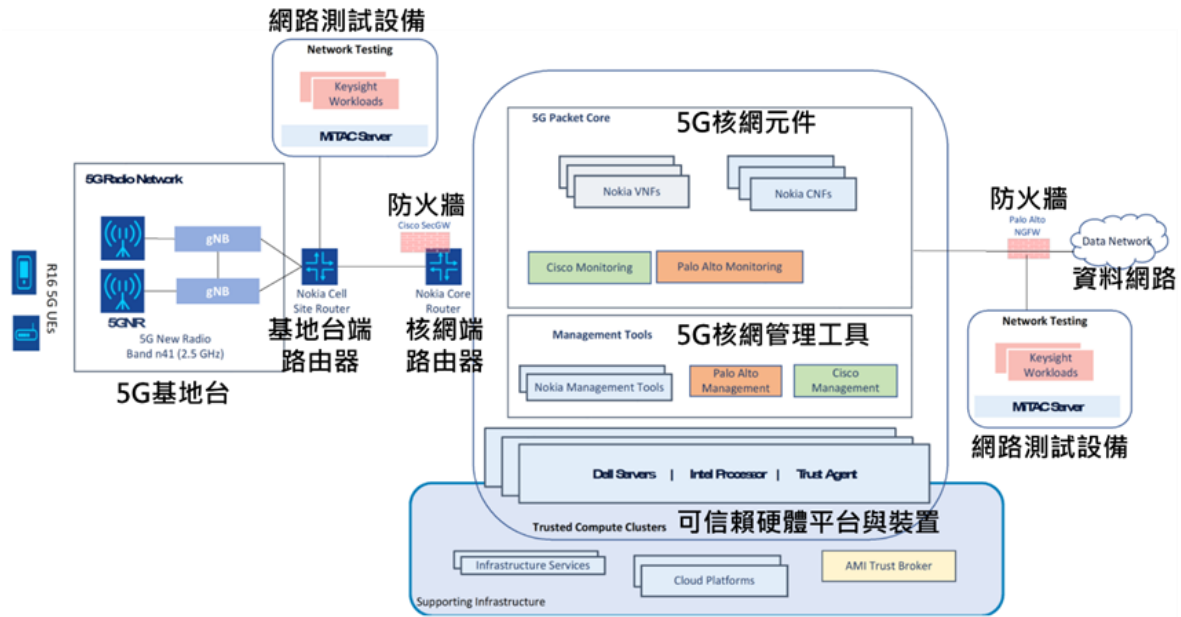


圖 62、5G 核網參考測試架構

資料來源：請參閱附錄-參考資料^{4.3}

透過上述的參考架構，可以進行 5G 核心網路的滲透測試關鍵項目包括：

- (一)NFV 測試：評估構成 5G 核網基礎設施虛擬化網路功能 (Virtualized Network Function, VNF)元件的安全性，以確保隔離並防止未經授權的訪問。
- (二)SDN 測試：評估 SDN 控制器和交換機的安全性，以及兩者之間的通訊，以確保網路的完整性和可用性。
- (三)身分驗證和授權測試：驗證用於保護 5G 核網元件和敏感資料存取的身分驗證和授權機制的穩健性(Robustness)。
- (四)互連安全測試：分析 5G 核網元件之間，例如 5G 基地臺(Next generation NodeB, gNB)的互連安全性，以防止未經授權的存取並保持網路的完整性。

4.3 NIST. (2022) NIST SPECIAL PUBLICATION 5G Cybersecurity. Retrieved from <https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf>



二、國內 5G IoT 滲透測試規範

台灣資通產業標準協會提出 IoT 場域資安防護評估指引(TAICS TR-0022 v2.0:2023)配合國家持續推動 IoT 技術及 5G 垂直應用之發展策略，研析國際 IoT 資安評估指引或規範，建立適用於 IoT 場域之資安評估機制。該指引審酌開放網頁應用程式安全專案(Open Web Application Security Project, OWASP)規範建立國內 IoT 場域滲透測試規範，該指引對於未來 6G 時代萬物聯網(Internet of Everything, IoE)的應用情境將可作為參考。該指引針對應用層、網路層、感測設備層提出 17 項滲透測試(Penetration Testing, PT)項目、15 項滲透情境(Infiltrate Situation, IS)，涵蓋 24 項安全控制項目(Security Controls, SC)，其整合如表 29 至表 31。

表 29、應用層滲透測試項目與基準

測試項目	測試基準	滲透情境	安全控制項目
PT01 網站應用程式弱點	網站應用程式應不可存有最新版本之 OWASP Top 10 可利用之風險。	IS01, Code Change	SC06
		IS02, Argument Change	SC07
		IS02, Argument Change	SC14
		IS02, Argument Change	SC15
		IS03, Data Change	SC16
		IS03, Data Change	SC26
		IS04, Privilege Change	SC27
		IS04, Privilege Change	SC32
PT02 網站設定管理	備份或測試檔案機敏資訊停用危險的 HTTP Method。啟用 HSTS (HTTP StrictTransport-Security) Header。	IS05, Service Change	SC28
		IS05, Service Change	SC30
		IS03, Data Change	SC34
		IS03, Data Change	SC35
			SC36
			SC40



測試項目	測試基準	滲透情境	安全控制項目
PT03 使用者通行碼強度	無使用常見對外服務之弱通行碼。	IS01, Code Change IS02, Argument Change IS03, Data Change IS04, Privilege Change	
PT04 使用者鑑別	鑑別過程已透過加密通道進行傳送。 瀏覽器無啟用通行碼儲存功能。	IS01, Code Change IS02, Argument Change IS03, Data Change IS04, Privilege Change	
PT05 使用者授權	目錄跨越弱點。 不同使用者的授權機制。 不同使用者的權限控管機制。 不安全物件參考弱點。	IS03, Data Change IS04, Privilege Change IS05, Service Change	
PT06 伺服器連線管理	Session 管理測試。 Cookie 屬性測試。 Session 資料更新測試。 Session 變數傳遞測試。 Session Timeout 測試。	IS02, Argument Change IS03, Data Change IS04, Privilege Change	



測試項目	測試基準	滲透情境	安全控制項目
		IS05, Service Change	
PT07 威脅 輸入驗證	測試 Cross-Site Scripting 弱點。 測試 Injection 弱點。 測試偽造 HTTP 協定。	IS01, Code Change IS02, Argument Change IS03, Data Change IS04, Privilege Change IS05, Service Change	
PT08 邏輯 漏洞	網站功能測試。 網站功能設計缺失測試。 檔案上傳測試。	IS01, Code Change IS02, Argument Change IS03, Data Change IS04, Privilege Change	
PT09 敏感 性資料檢測	確認網路傳輸過程無敏感性資料，如：帳號、通行碼、API Tokens、設定檔、程式原始碼、金鑰等	IS08, Data Change	SC05 SC07 SC14 SC15
PT10 身分 驗證機制	機敏性服務需提供身分驗證機制，如：每次登入需輸入帳號及通行碼	IS01, Code Change IS02, Argument Change	SC16 SC17 SC28 SC30 SC31



測試項目	測試基準	滲透情境	安全控制項目
		IS03, Data Change	SC32 SC34
		IS04, Privilege Change	SC35 SC36
			SC40

資料來源：請參閱附錄-參考資料^{4.3}

表 30、網路層滲透測試項目與基準

測試項目	測試基準	滲透情境	安全控制項目
PT11 加密通道測試	網路封包有無加密。	IS08, Data Change IS09, Privilege Change	SC06 SC07 SC15 SC17
PT12 無線射頻分析	Bluetooth 封包分析。 Zigbee 封包分析。 Wi-Fi 安全性協定測試。 無線通訊協定封包分析。	IS07, Code Change IS08, Data Change IS10, Service Change	SC26 SC32 SC33 SC34 SC35 SC36
PT13 連線管理	未開啟不安全的連接埠。 未經授權的存取頁面、連接，如： 不經鑑別就可連線的 SSH、FTP 或 Web-Console。	IS07, Code Change IS09, Privilege Change IS10, Service Change	SC37

4.3 台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會 (2023) 物聯網場域資安防護評估指引 v2



測試項目	測試基準	滲透情境	安全控制項目
PT14 伺服器傳輸鑑別	使用可信任之伺服器憑證。 資料傳輸需採用 TLS v1.2 以上之加密連線機制。 存取具有機密性資料須經過鑑別。	IS07, Code Change IS08, Data Change	

資料來源：請參閱附錄-參考資料^{4.3}

表 31、感測設備層滲透測試項目與基準

測試項目	測試基準	滲透情境	安全控制項目
PT15 韌體更新安全性	具備韌體更新機制。 檢測從遠端更新伺服器下載韌體更新檔時，是否進行傳輸加密。 韌體檔案未存有機敏性資訊。	IS11, Code Change IS12, Argument Change IS14, Privilege Change IS15, Device Change	SC08 SC09 SC10 SC11 SC13 SC15 SC16
PT16 更新檔安全性驗證	檢測韌體更新過程，是否對更新檔進行安全性驗證，如：更新來源、數位簽章、MD5 檢驗等。	IS11, Code Change IS14, Privilege Change IS15, Device Change	SC26 SC32 SC36 SC37
PT17 實體端口保護	檢測 IoT 裝置實體對外端口是否有限制存取，如：停用 USB 埠、使用實體鎖關閉等。	IS11, Code Change IS13, Data Change IS14, Privilege Change	

4.3 台灣資通產業標準協會—TC5 網路與資訊安全技術工作委員會 (2023) 物聯網場域資安防護評估指引 v2



測試項目	測試基準	滲透情境	安全控制項目
	檢測 IoT 裝置無法輕易解體或取出可卸除式儲存設備。	IS15, Device Change	

資料來源：請參閱附錄-參考資料^{4.3}

三、OWASP 滲透測試規範

OWASP 是一個國際性的組織，專門關注網頁應用的安全性。OWASP 提供許多資源、工具、指南和研究，幫助組織確保網頁應用程式的安全性。

OWASP Testing Guide 是 OWASP 提供的一個規範文件，主要焦點在於網頁應用程式的滲透測試。OWASP Testing Guide 提供明確、全面的滲透測試框架，覆蓋從資訊收集到身分認證、會話管理和各種網頁應用的常見漏洞。OWASP Testing Guide 分為多個部分，每部分專注於特定的測試領域，例如：身分驗證測試、會話管理測試、資料驗證測試等，以下是一些主要的測試項目及其簡要說明：

(一) 資訊蒐集

主要是做「目標偵測」，像是找出網站的 IP、子網域、使用的技術堆疊等，這可以幫助更了解目標網站的運作環境。

(二) 業務邏輯測試

主要是確認網站或應用程式在執行業務流程時，是否有可能被不正當地利用或繞過。如一個購物網站的折扣邏輯是否可以被濫用，導致不應該得到的優惠。

(三) 身分認證測試

確保網站的登入機制是安全的，無法被猜測密碼或利用漏洞繞過登入。



(四)Session 管理測試

檢查網站如何管理使用者的 Session，例如 Cookies 是否有適當地設定安全屬性，避免被劫持。

(五)資料驗證測試

檢查網站如何處理來自使用者的輸入，確保不會受到像是結構化查詢語言 (Structured Query Language, SQL) 注入、跨站腳本攻擊 (Cross-Site Scripting, XSS) 等威脅。

(六)基礎架構測試

檢視伺服器、資料庫或其他後端組件的配置，確保沒有暴露不必要的服務或接口。

(七)加密測試

確認網站在傳輸和儲存敏感資料時，是否都有使用適當的加密技術，例如保全超文字傳送協定 (Hypertext Transfer Protocol Secure, HTTPS)、資料庫加密等。

(八)客戶端測試

檢查像是瀏覽器或應用程式端的安全性，確保其不會成為攻擊的切入點，例如確保網頁不會執行不安全的 JavaScript。

這些測試項目都是為了確保網站和應用程式在面對各種威脅時，能保持其安全性和完整性。

第三節 6G 應用服務層之偵防工具化可行性評估

本計畫研究觀察 6G 與 5G 在網路威脅方面的差異，以釐清 6G 資安需求，針對 6G 網路 5 種攻擊，分別為 AI-Native 攻擊、in-X 子網 Network Slicing Security、IP Spoofing、DoS、Downgrade Attack 等資安威脅進行研究，了解攻擊手法、防禦、緩解措施及偵防工具，期望藉由本工作項目之研析，以提升政府情資分享架構在 6G 環境之可用性。

一、AI-Native 攻擊 (AI-Native Security)

(一)AI-Native 攻擊簡介

從部署和配置到管理，AI 有望在 6G 網路中發揮越來越大的作用，這種對 AI 依賴增加也將導致新的安全威脅，稱為 AI-Native 攻擊。

(二)AI-Native 攻擊原理

AI-Native 攻擊是專門針對 6G 網路的 AI 組件攻擊，這些攻擊可以利用 AI 軟體或硬體的漏洞，也可以使用 AI 技術來規避傳統安全防禦。AI-Native 攻擊包括：

1. 攻擊 AI 訓練資料

攻擊者破壞 AI 訓練資料，從而導致 AI 做出錯誤決定。

2. 攻擊 AI 軟體

攻擊者利用 AI 軟體中的漏洞來控制 AI 或破壞其運行。

3. 攻擊 AI 硬體

攻擊者可以物理損壞 AI 硬體，從而使 AI 無法使用。

4. 利用 AI 規避傳統安全防禦

攻擊者利用 AI 技術規避傳統安全防禦，例如防火牆和入侵偵測系統(Intrusion-Detection System, IDS)。

對 AI 的依賴增加將使 6G 網路更容易受到攻擊，而攻擊者使用 AI 技術將使攻擊更難防禦。為降低 AI-Native 攻擊的風險，6G

網路在設計時需要考慮到安全性，包括使用安全的 AI 軟體和硬體，以及實施檢測和防止 AI-Native 攻擊的安全措施。

(三)6G 情境下 AI-Native 攻擊緩解措施

為緩解 6G 網路中與 AI-Native 攻擊相關的安全威脅，可以考慮以下幾種措施：

1. 強大的 AI 模型測試和驗證

應對 AI 模型進行徹底測試和驗證，以識別、解決漏洞和潛在的攻擊向量，包括對抗性測試、資料清理和模型穩健性分析等技術。

2. 安全 AI 模型訓練

在訓練階段實施安全措施，例如資料完整性檢查、存取控制和安全資料儲存，有助於防止資料中毒和未經授權的修改。

3. AI 系統監控

持續監控 AI 系統和演算法，檢測異常行為、潛在攻擊或預期性能的偏差。監控可能涉及分析 AI 演算法的輸入、輸出和中間狀態，以識別篡改或對抗活動的跡象。

4. 安全資料管理

應採用強大的資料保護措施，包括加密、存取控制和隱私保護技術，以保護 AI 系統使用的敏感資料。

5. 對抗性防禦機制

開發和部署針對對抗性攻擊的強大防禦，例如檢測和過濾對抗性輸入，可以增強 AI 系統的彈性。

(四)AI-Native 的偵防工具

AI-Native 檢測和緩解工具，利用 ML、DL 和其他 AI 技術來檢測和響應各種類型的網路威脅。這些工具使用 AI 演算法來分析

大量數據，識別模式、異常和潛在威脅，並採取自動化措施來緩解這些威脅。以下介紹一些常用軟體：

1. Darktrace

Darktrace 的企業免疫系統使用 AI 來檢測和響應高級網路威脅，包括內部威脅、零時差攻擊等。透過收集設備或使用行為，並解構出獨有的行為模型，判定威脅與判斷異常行為，進行資訊安全鑑識與調查。

2. Vectra AI

Vectra 的網路檢測和響應 (Network Detection and Response, NDR) 平臺使用 AI 實時檢測威脅，確定威脅優先級。提供對網路流量中隱藏威脅的可見性並自動進行威脅搜尋。

3. CylancePROTECT

以人工智慧驅動的端點保護解決方案，使用 ML 來執行惡意威脅的防護。它根據行為分析阻止惡意軟體、勒索軟體和其他攻擊。

4. SentinelOne

人工智慧驅動的端點安全平臺，使用行為模型和 ML 來及時檢測和響應威脅。它可以自主減輕威脅及損害。

5. McAfee MVISION

McAfee 的安全平臺利用 AI 和 ML 來檢測和防止各種攻擊媒介（包括端點、網路、雲端和電子郵件）的威脅。

6. CrowdStrike Falcon

Falcon 的人工智慧驅動平臺提供端點保護、威脅情報和事件響應，通過分析行為模式實時檢測並阻止威脅。

7. Exabeam

Exabeam 的安全性資訊與事件管理(Security information and event management, SIEM)解決方案融合 AI 和 ML，可實現高級威脅檢測、內部威脅監控和自動事件響應。

8. FireEye Helix

FireEye 的平臺結合人工智慧驅動的分析、威脅情報和編排，幫助檢測、調查和響應網路威脅。

9. IBM QRadar

IBM 的 SIEM 解決方案使用 AI 和 ML 來提供高級威脅檢測、風險管理和事件響應功能。

10. Securonix

Securonix 的 SIEM 平臺使用使用者行為分析(User and Entity Behavior Analytics, UEBA)和 ML 來檢測內部威脅和網路攻擊。

值得注意的是，將 AI 整合到 6G 網路中及相關安全威脅仍在不斷發展的研究領域。隨著 6G 技術的進步，可能會出現對具體風險和相應安全措施的進一步了解。持續研究、行業合作和標準化工作對於解決 6G 網路中 AI-Native 攻擊帶來的安全挑戰至關重要。

二、In-X 子網 Network Slicing Security

(一)網路切片(Network Slicing)簡介

網路切片是將一個物理網路，切割成多個虛擬端到端的網路，每個虛擬網路之間，包括網路內的設備、接入、傳輸和核心網，是邏輯獨立的。任何一個虛擬網路發生故障，都不會影響到其他虛擬網路。

(二)網路切片原理

本質上，每個單獨的端到端網路切片都具有完整網路功能，包括特定的網路層功能、操作參數和網路特性。當然，每個人都有自

己的資源需求，例如運算、儲存或網路。一旦部署，就被稱為「網路切片實例」，其中每個切片至少有一個實例，它定義切片的行為，可以根據所選的切片向企業客戶提供一個或多個實例。如圖 63 所示。

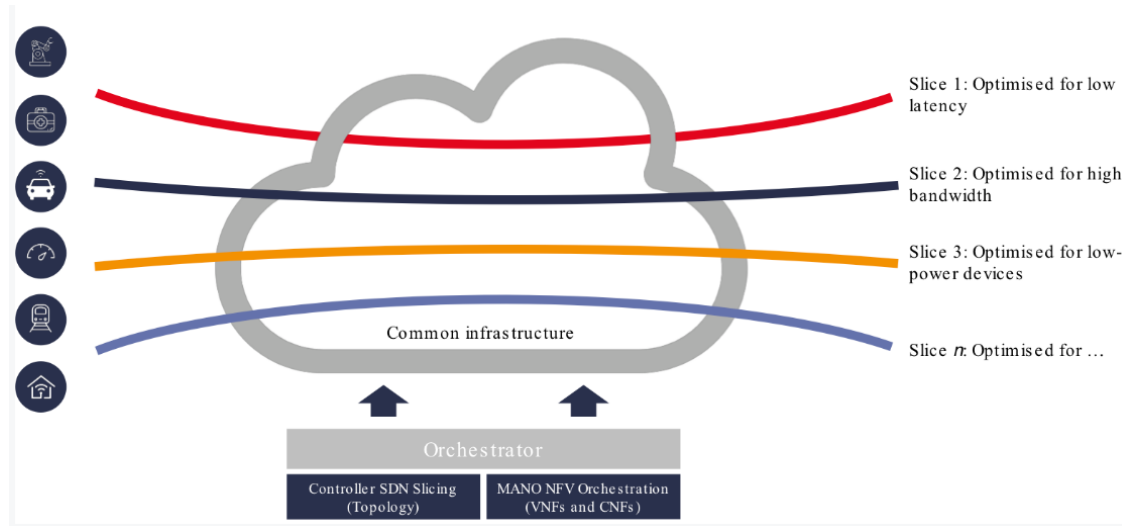


圖 63、網路切片的工作原理

資料來源：請參閱附錄-參考資料^{4.5}

每個網路切片都可以有不同的網路要求，具體取決於目標，它定義網路切片實例在其整個生命週期中的結構、配置和工作流。例如在 6G 的背景下，大規模連接 IoT 設備的客戶，如監控智慧電錶的公用事業公司，針對大規模機器進行更優化的切片—mMTC，而涉及自動駕駛汽車的應用程式需要針對 uRLLC 進行優化的切片。

網路切片帶給電信營運商和企業客戶巨大的價值，對於前者，主要歸結為服務敏捷性、靈活性和客製化解決方案：

1. 服務敏捷性

將網路切片視為電信公司專用網路服務選項的關鍵部分，企業客戶無需使用專用的行動網路，而是可以使用適合其特定連接要求的一個或多個網路切片。切片的概念可以為

4.5 "What is 5G network slicing?" Retrieved from <https://stlpartners.com/articles/private-cellular/what-is-5g-network-slicing/>

不同服務提供虛擬網路的邏輯分離，允許不同團隊在合適的地方管理和實施變化，且彼此獨立，例如某個團隊想要推出一項與當前核心服務截然不同的新服務，無需每次都重新設計整個網路。從而縮短上市時間並降低部署成本，使營運商能夠以更快的方式部署新服務以滿足客戶需求。

2. 靈活性

根據用定製網路特性的能力，意味著不同於過去幾代蜂巢式網路所採用的「一刀切」方法。最終，能夠滿足更廣泛客戶群特定需求的解決方案，無論是在不同的行業或地區，例如對於網路切片，想要定製網路特性且比公共雲提供網路更好的安全功能，企業客戶現在可以選擇網路切片而不是整個私有網路解決方案。

3. 解決方案

網路切片也作為一種「修剪」過去蜂巢式網路「臃腫」特性的方法，通過「一刀切」方法，整個網路被填滿以包括每一個功能和能力，以提供每一種可能發生的情況，並同時支援所有潛在的應用程式。通過網路切片，營運商可以根據最終定製網路，有效地「削減」不必要的功能，並利用節省下來的資金添加新技術，更好地滿足客戶需求，甚至提供更具競爭力的定價模式，例如 IoT 感測器的應用程式不需要圍繞行動或語音通訊的功能，這些功能會承擔不必要的成本，但可以從降低功耗的技術中獲益。

將這些結合在一起，網路切片是機會的核心，如果處理得當，網路切片在電信生態系統中具有巨大潛力。然而，它也將促成並要求營運商的業務和營運模式發生變化，以支援和促進切片的動態方面，網路切片可以在何時何地加速、擴大、縮小和退役需要。

5G 和 6G 網路切片都是允許在單個物理網路上創建多個虛擬網路的技術，但 2 種技術之間存在一些關鍵差異。

5G 網路切片旨在支持各種不同的服務，包括 eMBB、mMTC 和 uRLLC，每項服務在頻寬、延遲和可靠性方面都有自己的一套要求。網路切片允許為每個服務創建單獨的虛擬網路，確保每個服務都能獲得滿足其要求所需的資源。

6G 網路切片有望比 5G 網路切片更加靈活和動態。在 6G 中，網路切片將能夠按需求創建和銷毀，並且能夠調整大小以滿足用戶不斷變化的需求，將允許更有效地使用網路資源，並將支持更廣泛的應用。表 32 總結 5G 和 6G 網路切片之間的主要區別：

表 32、5G 和 6G 網路切片區別一覽表

特徵	5G 網路切片	6G 網路切片
支援的服務	eMBB, mMTC, uRLLC	eMBB, mMTC, uRLLC 等
靈活性	不太靈活	更靈活
動態	較少動態	較多動態
資源效率	效率較低	效率較高
應用支援	應用範圍廣	應用範圍更廣

資料來源：Google Bard 整理

總體而言，6G 網路切片有望成為比 5G 網路切片更先進、更靈活的技術。這將允許更有效地使用網路資源，並將支持更廣泛的應用程式。

(三)網路切片攻擊

網路切片提供一種新的攻擊向量來執行 DDoS 如圖 64 所示，有 2 個切片為 2 個提供服務不同類別的設備(即行動設備和 IoT 設備)，通用控制網路功能(Common Control Network Functions, CCNF)在 2 個切片之間共享並提供切片選擇和認證功能。

在這種情況下，有一個嘗試通過身分驗證的 IoT 設備數量切片 Slice#2。這可能會導致對 Slice#2 的 DDoS 攻擊組件。但是，兩者切片在核心網路中共享相同的物理鏈路(所有或 2 個切片的某些組件可以共享相同物理鏈接)，那麼 Slice#1 可能會受到影響，並且可能導致 Slice#1 上的間接 DoS。

1. 攻擊者建立大量的 IoT 殭屍網路。
2. 攻擊者指揮 IoT 殭屍網路同時對切片進行認證，淹沒網路資源。

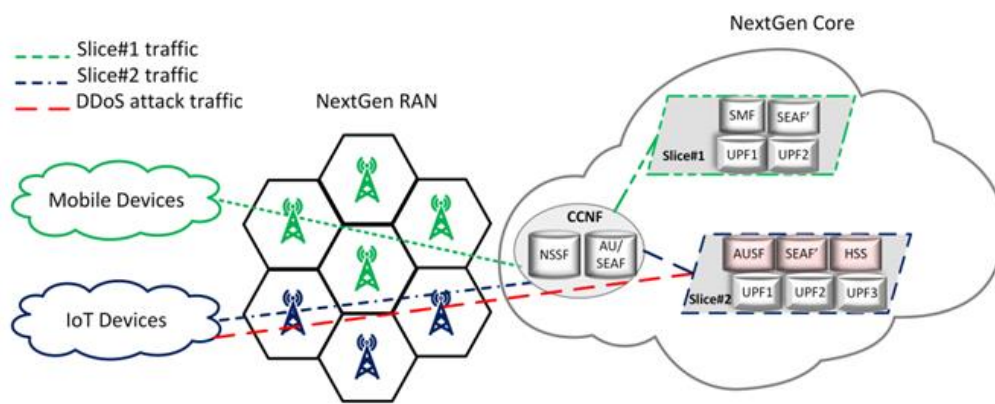


圖 64、網路切片攻擊原理

資料來源：請參閱附錄-參考資料^{4.6}

(四)網路切片防禦

通過採取以下步驟，網路營運商可以幫助保護 5G 和 6G 網路切片部署免受攻擊。

1. 使用強大的安全措施：包括使用強大的密碼、加密和存取控制。
2. 使軟體保持最新狀態：軟體更新通常包括有助於防範已知漏洞的安全更新檔。

4.6 Danish Sattar, Ashraf Matrawy. (2019). Trinity: Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices. Retrieved from <https://arxiv.org/pdf/1901.01443.pdf> (Jul. 03, 2023)

3. 了解最新的威脅：網路營運商應該及時了解最新的威脅和漏洞，以便採取措施來緩解。

5G 網路切片攻擊可能會被用來攻擊 6G 網路切片。然而，6G 也有可能包含新的安全功能，使其更能抵抗攻擊，例如 6G 有望使用比 5G 更先進的加密技術，這將使攻擊者更難攔截和解密流量。6G 也有望使用更複雜的身分驗證機制，這將使攻擊者更難獲得對網路切片的未授權存取。

但是，現在斷言 5G 網路切片攻擊是否可以用來攻擊 6G 網路切片還為時過早。6G 的安全性還在開發中，有可能會發現新漏洞。因此，網路營運商必須了解最新的威脅並採取措施緩解這些威脅。

(五)網路切片的偵防工具

有許多網路切片檢測和緩解工具可用，如下：

1. NetSlicer

一款開源工具，可用於檢測和緩解網路切片攻擊。NetSlicer 的工作原理是監視網路流量是否存在惡意活動，例如具有欺騙性源 IP 地址的數據封包或違反特定切片帶寬限制的數據封包。

2. NetCloak

一種商業工具，可用於檢測和緩解網路切片攻擊。NetCloak 通過結合使用 ML 和異常檢測等技術來識別惡意活動。

3. Flowmon

一種商業工具，可用於檢測和減輕網路切片攻擊。Flowmon 的工作原理是監控網路流量是否存在異常，例如流量峰值或不遵循預期模式的流量。

4. FortiGuard 網路切片安全

一種商業工具，可用於檢測和減輕網路切片攻擊。

FortiGuard 網路切片安全使用 ML 和異常檢測等多種技術來識別惡意活動。

5. Palo Alto Networks WildFire

一款商業工具，可用於檢測和減輕網路切片攻擊。Palo

Alto Networks WildFire 使用 ML 和沙箱等多種技術來識別惡意活動。

三、IP 欺騙 (IP Spoofing)

(一)IP Spoofing 簡介

IP Spoofing 是指創建具虛假源 IP 地址的 IP 封包，以冒充另一個電腦系統。IP Spoofing 允許網路犯罪分子執行惡意操作，而且通常不會被發現，這可能包括竊取資料、用惡意軟體感染設備或使伺服器崩潰。

是一種特定類型的網路攻擊，其中有人試圖使用電腦、設備或網路偽裝成合法實體來欺騙其他電腦網路。IP Spoofing 是駭客用來獲取設備存取權以挖掘敏感資料、將設備變成殭屍(被接管用於惡意用途的設備)或發起 DoS 攻擊的眾多工具之一，為最常見騙類型。

(二)IP Spoofing 原理

電腦網路通過交換網路封包進行通訊，每個封包包含多個用於路由和確保傳輸連續性的標頭，其中一個標頭是「源 IP 地址」，它指示封包發送方的 IP 地址。

IP Spoofing 係指駭客將假 ID 偽裝攻擊者的原始 IP，允許駭客使用虛假 IP 地址來隱藏身分和設備的真實來源。通過 IP Spoofing，駭客可以用惡意軟體感染設備、竊取敏感資訊或用 DDoS 攻擊淹沒網站。

駭客可以使用工具修改發送的 IP 封包源地址。使用虛假的源地址，在網路上看起來像一個受信任的設備，然後請求設備免費提供敏感資訊，獲得信任後駭客可以直接攻擊設備。IP 地址欺騙攻擊可能難以檢測，發生在沒有任何外在的篡改跡象，由於源地址是虛假和隨機的，因此很難阻止惡意請求或將欺騙攻擊追溯到實際來源。

IP Spoofing 攻擊期間，駭客會更改其 IP 地址以誘使設備誤認為合法的網站或程式，使用這種 IP Spoofing 方法，中間人駭客可以攔截 2 個設備之間的通訊，以便悄悄地更改或竊取 IP 封包，設備還可能將敏感資料隨意提供給中間人駭客，並在暗網市場上使用或出售這些資料。IP Spoofing 攻擊的工作原理如圖 65 所示：

1. 冒充受害者 IP 送封包到 Web Server。
2. Web server 回復訊息到受害設備，以虛假身分執行惡意活動。

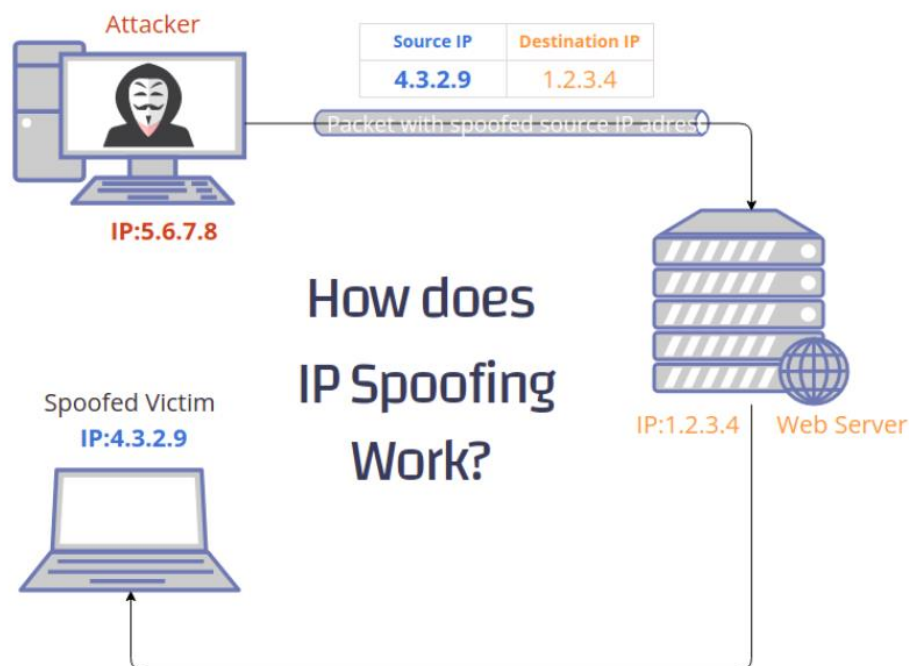


圖 65、IP Spoofing 攻擊的工作原理

資料來源：請參閱附錄-參考資料^{4.7}

4.7 What is IP Spoofing?. Retrieved from <https://www.zenarmor.com/docs/network-security-tutorials/what-is-ip-spoofing> (Jul. 03, 2023)

(三)IP Spoofing 攻擊類型

IP Spoofing 可用於多種攻擊，一旦駭客獲得設備的信任，就可以利用該漏洞請求個人資料、發送電腦病毒，甚至將設備變成殭屍以支援對目標網路的大規模機器人攻擊，其 IP Spoofing 攻擊的類型如下：

1. DDoS 攻擊

在 DDoS 攻擊中，駭客使用欺騙性 IP 地址封包淹沒電腦伺服器，使駭客能夠隱藏身分的同時崩潰具有大量網際網路流量的網站或網路。在 DDoS 攻擊中使用 IP 地址欺騙有「掩蓋殭屍網路設備位置」和「進行反射攻擊」2 個原因。

(1)屏蔽殭屍網路設備：

殭屍網路是一組受惡意軟體感染的設備，由犯罪者在所有者不知情的情況下遠端控制，為犯罪者提供運算和網路資源以產生巨大的流量洪流，導致伺服器停機和網路飽和。殭屍網路通常由隨機、地理上分散的設備或屬於同一受感染網路(如被黑的託管平臺)的電腦組成，通過使用欺騙性 IP 地址來掩蓋其殭屍網路設備的真實身分，犯罪者旨在避免被執法部門和法醫網路調查人員發現和牽連、防止目標通知設備所有者無意中參與的攻擊、繞過試圖通過將攻擊 IP 地址列入黑名單來減輕 DDoS 攻擊的設備和服務。

(2)反射型 DDoS：

反射型 DDoS 攻擊使用 IP Spoofing 生成虛假請求，表面上代表目標，以從受保護的中間伺服器中引出反應。犯罪者目標是通過觸發來自更小請求的大反應來放大流量輸出。

2. 中間人攻擊(Men in the Middle Attack, MitM)

另一種惡意 IP Spoofing 方法使用 MitM 攻擊來中斷 2 臺電腦間的通訊，更改封包並在原始發送者或接收者不知情的情況下傳輸。如果駭客欺騙 IP 地址並獲得對個人通訊帳戶的存取權限，駭客就可以跟踪該通訊的任何方面，可能竊取資訊、將用戶引導至虛假網站等。隨著時間的推移，駭客會收集到大量可以使用或出售的機密資訊，這意味著 MitM 可能比其他攻擊更有利可圖。

5G IP Spoofing 可以用來攻擊 6G IP Spoofing。IP Spoofing 是一種允許攻擊者發送帶有虛假源 IP 地址的封包的技術。這可用於冒充另一臺設備或對網路發起攻擊。

6G 的安全特性還在開發中，所以有可能利用一些 5G IP Spoofing 攻擊來攻擊 6G。然而，6G 也有可能包含新的安全功能，使其更能抵抗 IP Spoofing 攻擊。例如 6G 有望使用更先進的認證機制，將使攻擊者更難獲得對網路的未授權存取。6G 也有望使用更複雜的流量監控和分析技術，有助於識別和阻止 IP Spoofing 攻擊。

但是，現在斷言 5G IP Spoofing 攻擊是否可以用來攻擊 6G IP Spoofing 還為時過早。6G 的安全性還在開發中，有可能會發現新的漏洞。因此，網路營運商必須了解最新威脅並採取措施緩解這些威脅。

為幫助防止 IP Spoofing，使用虛擬專用網路(Virtual Private Network, VPN)來隱藏 IP 地址，並使用防火牆監控網路是否存在可疑活動，防火牆使用檢查 IP 封包標頭的封包過濾器，只存取使用 HTTPS 的安全站點，確保盡可能使用高強度的密碼。

(四)IP Spoofing 防禦

IP Spoofing 不可能完全防止，但是可以採取一些措施來阻止欺騙性 IP 封包進入網路，以下工具有助於防止 IP Spoofing 攻擊：

1. 強大的驗證方法：SSL 證書等工具有助於驗證試圖連接到使用者網路的網站。
2. 防火牆：使用防火牆保護使用者的網路，以保護設備免受未經授權 IP 封包、虛假源 IP 地址和可疑流量的侵害。
3. 最新的網際網路協議：IPv6 與 IPv4 提供更新的安全保護。
4. HTTPS 網站：具有安全加密協議的網站通常更安全，在線安全瀏覽器擴展程式還可以幫助使用者在瀏覽時檢測危險網站。
5. 高強度的密碼：創建高強度的密碼有助於防止 IP 欺騙者進入使用者的設備。
6. IP 地址認證：使用 IP 地址身分驗證代替其他登錄資料可以幫助驗證用戶。
7. 值得信賴的殺毒軟體：通過使用市場上最好的防病毒應用程式之一，更可能抓住任何試圖潛入使用者網路的入侵者。

(五)IP Spoofing 的偵防工具

檢測和緩解 IP Spoofing 涉及識別攻擊者何時偽造網路數據封包中的源 IP 地址以欺騙系統或逃避安全措施。雖然沒有專門針對 IP Spoofing 的工具，但有各種網路安全工具和技術可以幫助檢測和減輕 IP 欺騙攻擊。以下是一些方法：

1. 反欺騙過濾

配置網路設備（路由器、交換機、防火牆）以丟棄源自內部網路源 IP 地址屬於外部網路的數據封包。這稱為出口和入口過濾。通過確保內部數據封包具有合法的內部源 IP 地址，以防止外部攻擊者注入欺騙性數據封包。

2. 反向路徑過濾

在路由器上實施單播反向路徑轉發(Unicast Reverse Path Forwarding, uRPF)。該技術檢查數據封包的源 IP 地址

是否可以通過其到達的接口到達。這有助於通過丟棄源 IP 無法通過預期接口到達的數據封包來防止 IP Spoofing 攻擊。

3. 網路入侵偵測系統 (Network Intrusion Detection System, NIDS)

NIDS (例如 Snort 或 Suricata) 可以配置為檢測表明 IP 欺騙的網路流量模式。例如，在短時間內觀察到多個子網上來自單個源 IP 地址的流量，則可能表明存在欺騙。

4. 深度包檢測 (Deep Packet Inspection, DPI)

DPI 工具深入分析網路流量，尋找可能表明 IP Spoofing 的不一致和模式。DPI 可以是 IDS 或入侵防禦系統 (Intrusion-Prevention System, IPS) 的一部分。

5. 流量分析

監控和分析網路流數據有助於檢測異常模式，包括 IP 欺騙實例。NetFlow 或 sFlow 收集器等工具可以幫助解決此問題。

6. 威脅情報

利用威脅情報源和數據庫提供有關已知惡意 IP 地址的信息，這可以幫助識別潛在的欺騙來源。

7. 加密與認證

使用網際網路安全協定 (Internet Protocol Security, IPsec) 等加密協議來確保數據封包的完整性並驗證發送者身分，有助於降低數據被攻擊者攔截和操縱的風險。

8. 網路分段

將網路分割成更小的子網並實施嚴格的訪問控制。這樣可以使 IP Spoofing 攻擊限制在的較小部分內，限制其影響。

9. 行為分析

監控網路設備和用戶的流量模式和行為。檢測到突然變化或偏離正常行為可能表明在進行 IP Spoofing 嘗試。

雖然這些工具和技術可以幫助檢測和緩解 IP Spoofing，但值得注意的是，由於網際網路架構的固有性質，完全消除 IP Spoofing 攻擊仍然具有挑戰性，結合這些措施的多層安全方法可以顯著降低 IP Spoofing 攻擊成功的風險。

四、Denial of Service

(一)DoS 簡介

DoS 是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常使用者無法存取。通常，透過大量的流量或請求使目標系統不堪重負，使其無法反應合法請求來實現，並阻止系統向其用戶提供預期的服務。

(二)DoS 原理

有多種方法可用於執行 DoS 攻擊，包括用大量流量淹沒目標系統(例如使用殭屍網路的受感染電腦網路)，利用目標系統中的漏洞使其崩潰，或針對關鍵基礎設施組件(例如路由器或伺服器)以阻止用戶正常運行如圖 66。

1. DoS 攻擊的工作原理

(1)攻擊者入侵設備建立殭屍網路。

(2)殭屍網路阻斷網路資源，使合法用戶無法存取。

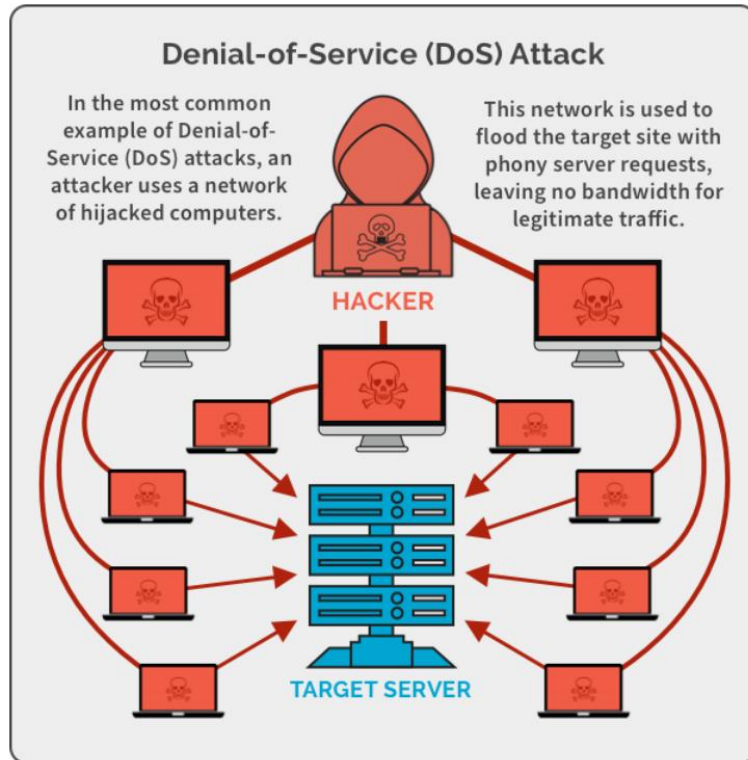


圖 66、DoS 攻擊的工作原理

資料來源：請參閱附錄-參考資料^{4.8}

2. DoS 攻擊的目的

- (1) 贖金：攻擊者通常在進行 DoS 攻擊後要求贖金。但是，有時也可以事先發送威脅攻擊的贖金通知。
- (2) 發表意見：DoS 攻擊也用於發表意見。駭客可以進行 DoS 攻擊，以表明對法規、個人或公司的支援或反對。
- (3) 競爭：超過 40% 遭受 DoS 攻擊的公司將其歸咎於競爭對手。

一旦確定遭受到 DoS 攻擊，迅速採取行動很重要，因為可以有機會防止嚴重的停機，如果等待時間過長，伺服器可能會開始崩潰，其 DoS 攻擊症狀包括：

4.8 Shyam Oza. Denial-of-Service (DoS) Attacks — Web-based Application Security, Part 7. Retrieved from <https://spanning.com/blog/denial-of-service-attacks-web-based-application-security-part-7/> (Jul. 03, 2023)

1. 網路異常緩慢(打開檔案或存取網站)
2. 特定網站無法存取
3. 無法存取任何網站
4. 垃圾郵件的數量急劇增加
5. 無線或有線網路連接異常
6. 伺服器容易斷線、卡頓、存取延遲

DoS 攻擊也可能導致目標電腦同一網路中的其他電腦被攻擊，網際網路和區域網路之間的頻寬會被攻擊導致大量消耗，影響目標電腦同時也影響區域網路中的其他電腦。如果攻擊的規模較大，整個地區的網路連接都可能會受到影響。迄今最大規模的 DoS 攻擊發生於 2017 年 9 月，該攻擊的目標是 Google 服務，規模達到 2.54 Tbps。

(三) 分布式反射拒絕服務攻擊(Distributed Reflection Denial of Service Attack, DrDos)

DrDoS 技術通常涉及多臺受害機器，受害者無意中參與針對攻擊者目標的攻擊。對受害主機的請求從受害主機重定向或反射到目標，通常攻擊者還會引發大量的攻擊流量。

攻擊者對暴露於網際網路的設備和伺服器上濫用以下協議來發起攻擊，這些攻擊會產生大量流量並導致企業目標的網站和網路中斷如圖 67：

1. DNS 用於在 IP 地址和網域之間進行轉換，允許用戶在瀏覽器中鍵入網址。
2. 網路時間協議(Network Time Protocol, NTP)用於網際網路伺服器的時間同步。
3. 攻擊者讓受害者主機伺服器看起來主要目標正在通過請求聯繫攻擊者。

4. 受害主機伺服器回應目標，錯誤地認為目標發出初始請求（欺騙）。

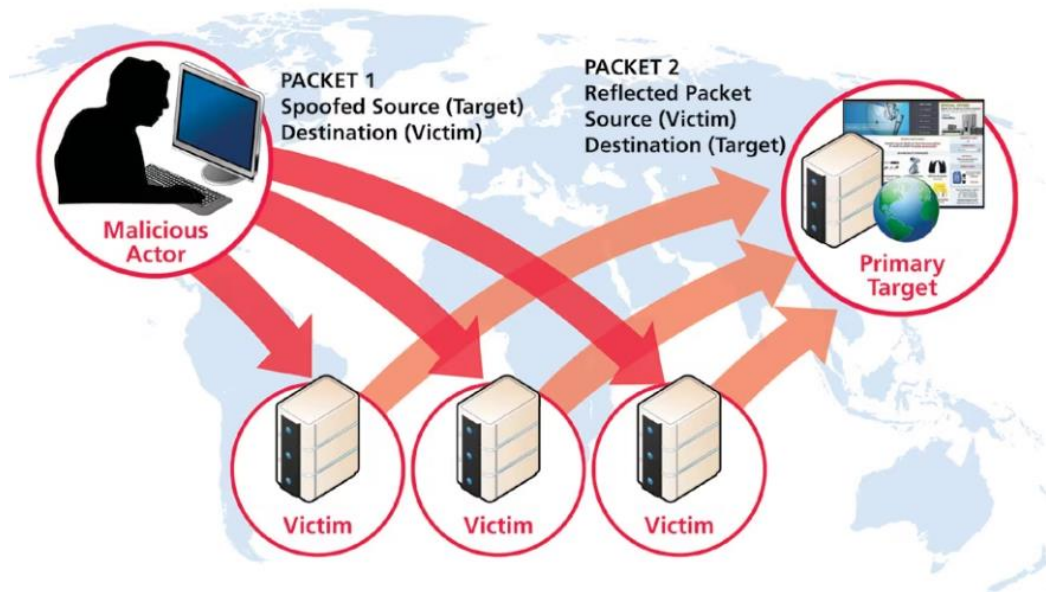


圖 67、DrDoS 攻擊的工作原理

資料來源：請參閱附錄-參考資料^{4.9}

5G 拒絕服務(DoS)攻擊可用於攻擊 6G DoS。DoS 攻擊是企圖使其目標用戶無法使用網路或服務，這可以通過向網路充斥流量、使伺服器過載或利用軟體中的漏洞來實現。

6G 的安全特性還在開發中，所以有可能利用一些 5G DoS 攻擊來攻擊 6G。然而，6G 也有可能包含新的安全功能，使其更能抵抗 DoS 攻擊，例如 6G 有望使用更先進的認證機制，這將使攻擊者更難獲得對網路的未授權存取。6G 也有望使用更複雜的流量監控和分析技術，這將有助於識別和阻止 DoS 攻擊。

現在斷言 5G DoS 攻擊是否可以用來攻擊 6G DoS 還為時過早。6G 的安全性還在開發中，有可能會發現新的漏洞。因此，網路營運商必須了解最新的威脅並採取措施緩解這些威脅。

4.9 DrDoS Attacks. Retrieved from <https://www.arturai.com/en/support/faqs/drDOS-attacks> (Jul. 03, 2023)

(四)DoS 防禦

DoS 攻擊的防禦方式通常為入侵檢測，流量過濾和多重驗證，旨在堵塞網路頻寬的流量將被過濾，而正常的流量可正常通過。防禦方式說明如下：

1. 防火牆

防火牆可以設定規則，例如允許或拒絕特定通訊協定埠或 IP 位址。當攻擊從少數不正常的 IP 位址發出時，可以簡單的使用拒絕規則阻止一切從攻擊源 IP 發出的通訊。複雜攻擊難以用簡單規則來阻止，例如 80 埠(網頁服務)遭受攻擊時不可能拒絕埠上所有的通訊，因為其同時會阻止合法流量。防火牆能有效地防止使用者從啟動防火牆後的電腦發起攻擊。

2. 交換機

大多數交換機有一定的速度限制和存取控制能力。有些交換機提供自動速度限制、流量整形、後期連接、DPI 和假 IP 過濾功能，可以檢測並過濾 DoS 攻擊，例如 SYN 洪水攻擊可以通過後期連接加以預防。基於內容的攻擊可以利用 DPI 阻止。

3. 路由器

和交換機類似，路由器也有一定速度限制和存取控制能力，而大多數路由器很容易受到攻擊影響。

4. 黑洞引導

黑洞引導指將所有受攻擊電腦的通訊全部傳送至一個「黑洞」(不存在的電腦位址)或者有足夠能力處理洪流的網路裝置商，以避免網路受到較大影響。

5. 流量清洗

當取得到流量時，通過 DoS 防禦軟體處理，將正常流量和惡意流量區分開，正常流量則回流回客戶網站，反之則封鎖。這樣一來能夠保持正常的運作，處理真實使用者存取網站帶來的合法流量。

DoS 緩解是一組技術，用於來抵抗或降低分散式 DoS 攻擊對受保護伺服器的影響。DoS 攻擊可以使目標伺服器效能降低甚至完全不可用，從而對企業和組織構成持續威脅。

(五)DoS 的偵防工具

有多種工具和解決方案可用於檢測和減輕 DoS 攻擊。這些工具旨在早期階段識別攻擊，然後採取措施減輕或最小化其影響。以下是一些常見的 DoS 檢測和緩解工具：

1. Arbor Networks Peakflow

Peakflow 平臺旨在提供實時網路可見性、威脅檢測和自動緩解 DDoS 攻擊。

2. Radware DefensePro

一種基於硬體的解決方案，用於檢測和緩解各種類型的 DDoS 攻擊，包括流量攻擊、應用層攻擊和 SSL 攻擊，使用行為分析和實時簽名創建來提供保護。

3. Cloudflare

提供基於雲端的 DDoS 防護服務，利用其廣泛的全球網路在攻擊流量到達伺服器之前對其進行過濾和緩解，可防禦各種類型的 DDoS 攻擊並提供實時攻擊分析。

4. Akamai Prolexic

提供一系列功能，包括流量清理、威脅情報以及用於實時監控和呼叫的安全營運中心。

5. Imperva Incapsula

基於其雲端的安全服務，包括 DDoS 防護、Web 應用程式防火牆和機器人緩解，提供分層安全性以防止各種攻擊。

6. Corero SmartWall

提供實時 DDoS 保護解決方案，使用實時資料封包檢測來識別和減輕 DDoS 攻擊，而不影響合法訪問的流量。

7. Check Point DDoS Protector

旨在針對網路和應用層 DDoS 攻擊提供高級檢測和緩解，運用行為分析和基於簽名的檢測來識別和阻止攻擊流量。

8. Fortinet Forti DDoS

可以識別和減輕網路層和應用層的攻擊，並提供 SYN Cookie 和速率限制等功能。

選擇 DoS 檢測和緩解工具時，須考慮多種因素，如可以處理的攻擊類型、可擴展性、與現有基礎設施銜接的難易程度以及供應商提供的支持和專業知識水準。並須定期更新和測試 DDoS 緩解策略，以確保其針對不斷發展的攻擊技術的有效性。

五、降級攻擊 (Downgrade Attack)

(一) Downgrade Attack 簡介

Downgrade Attack 是一種透過將受害者主機降級到有漏洞的舊版本，進行滲透、竊取機密或隱私資訊。在 Downgrade Attack 中，攻擊者故意使系統放棄新式、安全性高的工作方式(如加密連接)，反而使用為向下相容而準備的老式、安全性較差的工作方式(如明文通訊)。例如在 OpenSSL 中，曾經存在一個缺陷，從而使攻擊者能夠讓 SSL/傳送層安全協定(Transport Layer Security protocol, TLS)伺服器與用戶端建立老版本 TLS 連接，儘管雙方事實上支援新版本。

(二)Downgrade Attack 原理

現代 TLS 用戶端和伺服器支援舊版本的 TLS 協議與比較弱的加密演算法以實現向後相容，TLS Downgrade Attack 是攻擊者欺騙 TLS 用戶端和伺服器使用舊版本的 TLS 協議或比較弱的加密演算法或不安全參數的攻擊如圖 68。因此，攻擊者可以利用舊協議版本或弱密碼演算法或比較弱的安全漏洞來連接並竊取敏感資料。將 TLS 協議降級為 SSL 協議的攻擊手法如下：

1. 將 TLS 1.2 版降級到 SSL 3.0 版
2. 降級易暴露敏感訊息或未經授權存取

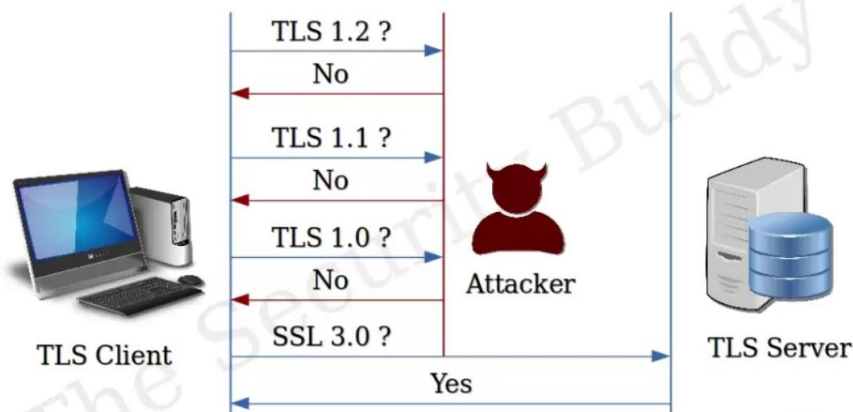


圖 68、TLS Downgrade Attack

資料來源：請參閱附錄-參考資料^{4.10}

為完成降級，常用策略是進行 MitM，有可能破壞用戶的網路活動，之後將利用用戶作為中間人的地位來進行 Downgrade Attack，攻擊者會誘騙伺服器使用保護程度較低的 TLS 或 SSL 版本。

降級完成後，攻擊者可以利用 MitM 來奪取顧客與伺服器之間的流量。儘管如此，它也可用於通過向伺服器發送虛假請求來故意

4.10 Amrita Mitra. (2020). What is TLS Downgrade attack? . Retrieved from <https://www.thesecuritybuddy.com/data-breaches-prevention/what-is-tls-downgrade-attack> (Jul. 03, 2023)/

破壞流量，以試圖竊取敏感資料，例如加密金鑰、會話 Cookie 或類似資料。

(三)Downgrade Attack 攻擊方式

Downgrade Attack 有很多種，可以根據以下屬性進行分類：

1. 元素：攻擊者試圖降級內容，協議本身的版本、其使用的加密演算法等。
2. 漏洞：是什麼讓攻擊成為可能，例如可能是對網路協議過時版本的過度支援。
3. 攻擊方法：為降低連接的安全級別，攻擊者可以修改建立安全連接的請求，重置它以便用戶端或伺服器嘗試建立不安全的連接，或者向其中一臺主機發送虛假的消息。

5G 網路 Downgrade Attack 可以用來攻擊 6G 網路。網路 Downgrade Attack 是試圖強制設備連接到較低頻寬的網路，可以通過向設備發送看似來自合法網路但實際上來自攻擊者的訊號來完成。

6G 的安全特性還在開發中，所以有可能利用一些 5G 網路降級來攻擊 6G。然而，6G 有可能包含新的安全功能，使其更能抵抗網路 Downgrade Attack，例如 6G 有望使用更先進的認證機制，將使攻擊者更難獲得對網路的未授權存取。6G 也有望使用更複雜的流量監控和分析技術，將有助於識別和阻止網路 Downgrade Attack。

不過，現在斷言 5G 網路 Downgrade Attack 是否可以用來攻擊 6G 還為時過早。6G 的安全性還在開發中，有可能會發現新的漏洞。因此，網路營運商必須了解最新的威脅並採取措施緩解威脅。

(四)Downgrade Attack 防禦

以下為緩解 6G 網路 Downgrade Attack 的方法：

1. 使用強大的安全措施：包括使用強大的密碼、加密和存取控制。

2. 使軟體保持最新狀態：軟體更新通常包括有助於防範已知漏洞的安全更新檔。
3. 了解最新的威脅：網路營運商應及時了解最新威脅和漏洞，以便採取措施來緩解攻擊。
4. 使用安全解決方案：安全解決方案可以幫助抵禦各種攻擊，包括網路 Downgrade Attack。
5. 實施網路安全最佳實踐：可以實施許多安全最佳實踐來幫助防止網路 Downgrade Attack，這些包括：
 - (1) 使用防火牆：防火牆可用於阻止未經授權的流量進入網路。
 - (2) 使用 IDS：IDS 用於檢測可疑流量並提醒網路營運商。
 - (3) 使用蜜罐：蜜罐旨在吸引攻擊者的誘餌設備。

通過採取這些步驟，網路營運商可以保護網路免受網路 Downgrade Attack。除了使用具體緩解技術將取決於網路面臨的具體威脅，但通過採用分層安全方法，網路營運商可以幫助保護其網路免受各種網路 Downgrade Attack。

(五) Downgrade Attack 偵防工具

有許多針對降級的檢測和緩解工具可使用，以下是為常見的使用工具：

1. Tripwire

一款開源的文件完整性檢查器，可用於檢測文件和目錄的更改，通過監視系統中對安全至關重要的文件更改來檢測 Downgrade Attack。

2. AIDE

一款開源的文件完整性檢查器，其與 Tripwire 類似，但有更多附加功能，例如檢測文件權限和所有權更改的能力。



3. OSSEC

一款開源 IDS，可用於檢測各種攻擊，包括 Downgrade Attack，可監控網路流量是否存在惡意活動，還可以用於監控系統中的日誌紀錄是否存在可疑活動。

4. Snort

一款可用於檢測 Downgrade Attack 的開源 IDS，其功能與 OSSEC 類似，提供更廣泛的特性和功能。

5. Suricata

一種較新型的 IDS，與 Snort 類似但相比具有更多優勢，例如支持更多協議以及檢測更新。

第四節 可支援 6G 網路威脅訊結構

一、STIX 簡介

STIX 是由 MITRE 公司(The MITRE Corporation)所定義與開發出用來快速能達到表示資安事件相關性與涵蓋性之語言，以表達出架構性的網路威脅資訊，用於規範、獲取、描述和傳達標準化網路威脅資訊，目前以 STIX 2.1 為最新版本。STIX 的使用情境如圖 69 所示：

- (一)UC1：分析網路威脅
- (二)UC2：將網路威脅特徵進行分類
- (三)UC3：管理網路威脅事件回覆行為
- (四)UC4：分享網路威脅資訊

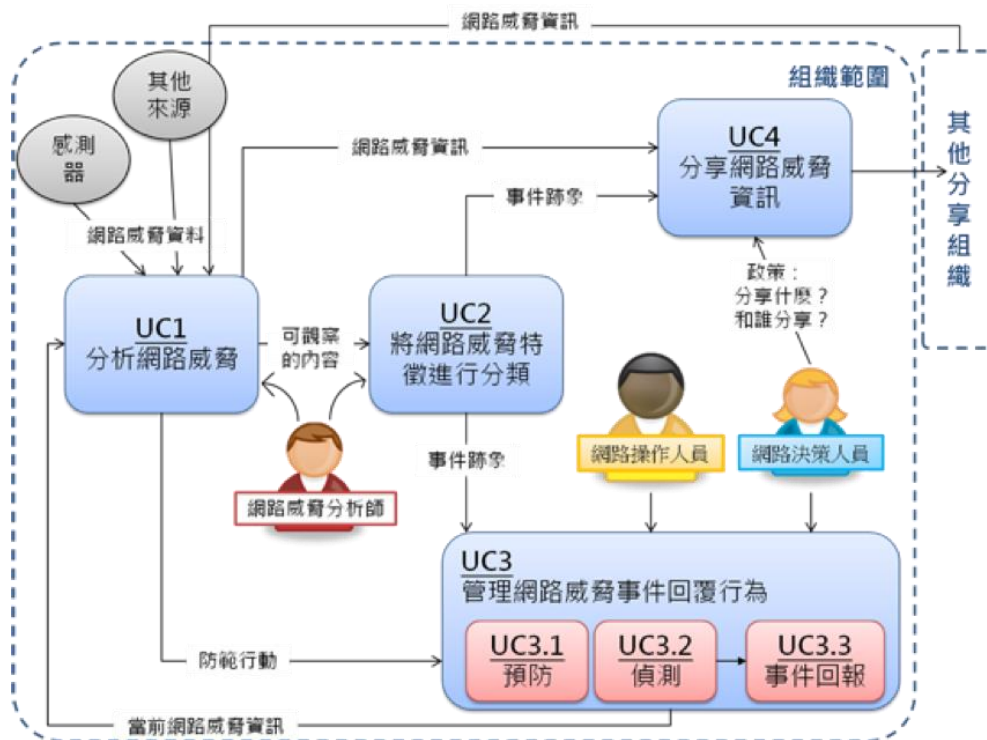


圖 69、STIX 的使用情境

資料來源：請參閱附錄-參考資料^{4.11}

4.11 "STIX (1)" (2018). Retrieved from <https://ithelp.ithome.com.tw/articles/10206720> (Jul. 03, 2023)

二、使用 STIX 單位

- (一)我國國家資安聯防監控中心(National Security Operation Center, N-SOC, Taiwan)
- (二)我國國家資安資訊分享與分析中心(National Information Sharing and Analysis Center, N-ISAC, Taiwan)
- (三)美國國土安全部-資通安全辦公室(Office of Cybersecurity and Communications, USA)
- (四)美國國家網路安全和通訊整合中心(National Cybersecurity and Communications Integration Center, USA)
- (五)美國電腦緊急應變小組(US-CERT, USA)

我國政府聯防監控依據公務機關回傳的資安監控情資，經過趨勢統計、分類分群及分析預測，建立政府資安情境認知，提供整體情報給 N-SOC，支援政府資安決策與推動公私資安協同合作，詳見圖 70。

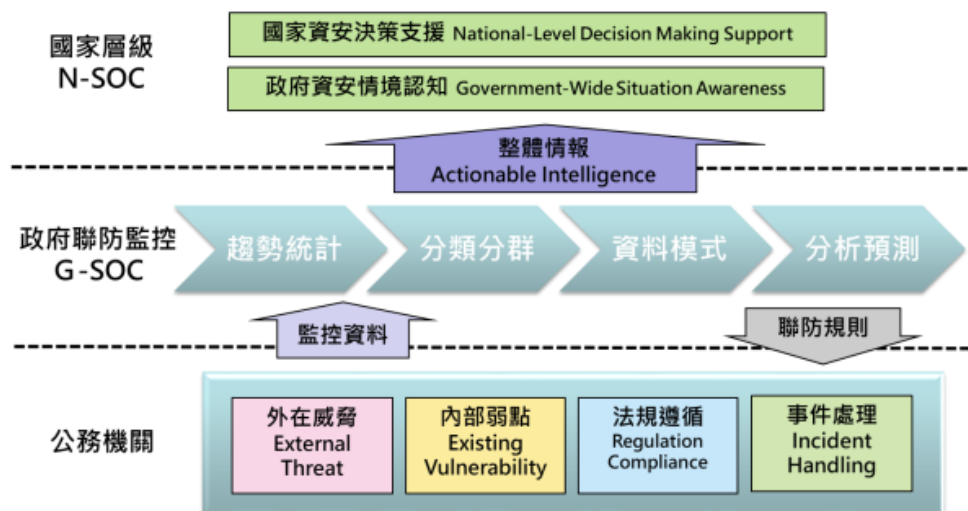


圖 70、各層級角色權責與分工

資料來源：請參閱附錄-參考資料^{4.12}

N-ISAC 情資以 JavaScript Object Notation(JSON)資料格式做為資料交換語言，並採用 STIX 格式為基礎，訂定 6 大情資種類。透過

4.12 國家資通安全研究院. <https://www.nics.nat.gov.tw/.htm> (Jul. 03, 2023)

情資格式之定義，整合國家資通安全會通報應變組下各通報應變分組之感測與通訊整合(Integrated Sensing and Communications, ISAC)所交換情資格式，經由指標資訊的可信自動交換(Trusted Automated eXchange of Indicator Information, TAXII)傳輸架構進行自動化情資交換，以遂跨組織之情資傳遞與交流，強化我國整體資安防護能量，並增進各關鍵基礎設施領域之情資分享與分析能力，落實推動跨領域資安聯防體系。

N-ISAC 參考 ENISA 所發表之 Information Sharing and Analysis Centers(ISACs)- Cooperative models 與 Reference Incident Classification Taxonomy，重新規劃 6 類資安情資種類與 10 類資安事件類型，並用以取代原先 N-ISAC 情資分類之 5 類(資安訊息情資、網頁攻擊情資、入侵攻擊情資、資安預警情資、回饋情資)，分類架構如圖 71 所示。



圖 71、6 類資安情資種類與 10 類資安事件類型

資料來源：請參閱附錄-參考資料^{4.12}

4.12 國家資通安全研究院. <https://www.nics.nat.gov.tw/.htm> (Jul. 03, 2023)



N-ISAC 6 類情資種類對應 STIX 2.1 欄位，分為資安事件與非資安事件，二者比較差異在項次 10 及 11 如圖 72 所示。資安事件是針對特定對象情資與特定對象所屬設備相關之資安事件。

資安事件對應之STIX 2.1欄位

項次	欄位名稱	STIX 2.1 物件(屬性)
1	情資來源	Identity(name)
2	情資編號	Grouping (labels)
3	情資分類	Grouping (context)
4	情資主旨	Grouping (name)
5	情資發布時間	Grouping (created)
6	影響等級	Grouping (x_severity)
7	內容說明	Grouping (description)
8	參考資訊	說明
	網址	Grouping (external_reference)(source_name)
9	分享等級	Grouping (external_reference)(url)
10	攻擊 IP	Marking Definition(name)
11	受駭 IP	Infrastructure consists-of IPv4 Address Object(value)
12	建議措施	IPv4 Address Object(value)
13	附件	Course of Action(description)
		Artifact Object

5類非資安事件對應之STIX 2.1欄位
(漏洞公告、威脅預警、態勢感知、最佳實務、策略分析、系統服務訊息)

項次	欄位名稱	STIX 2.1 物件(屬性)
1	情資來源	Identity(name)
2	情資編號	Report(labels)
3	情資分類	Report(report_types)
4	情資主旨	Report(name)
5	情資發布時間	Report(published)
6	影響等級	Report(x_severity)
7	內容說明	Report(description)
8	參考資訊	說明
	網址	Report(external_reference)(source_name)
9	分享等級	Report(external_reference)(url)
10	影響平台-系統	Marking Definition(name)
11	影響平台-軟體	Identity(name)
12	建議措施	Software(name)
13	附件	Course of Action(description)
		Artifact Object

圖 72、N-ISAC 情資欄位對應 STIX 2.1 物件說明(資安事件與非資安事件)

資料來源：請參閱附錄-參考資料^{4.12}

N-ISAC 以適當之 STIX 2.1 物件制定情資格式，依情資種類需求訂定 4 種情資格式基本架構，資安事件的情資格式架構代碼為 1，如圖 73 所示。

4.12 國家資通安全研究院. <https://www.nics.nat.gov.tw/.htm> (Jul. 03, 2023)

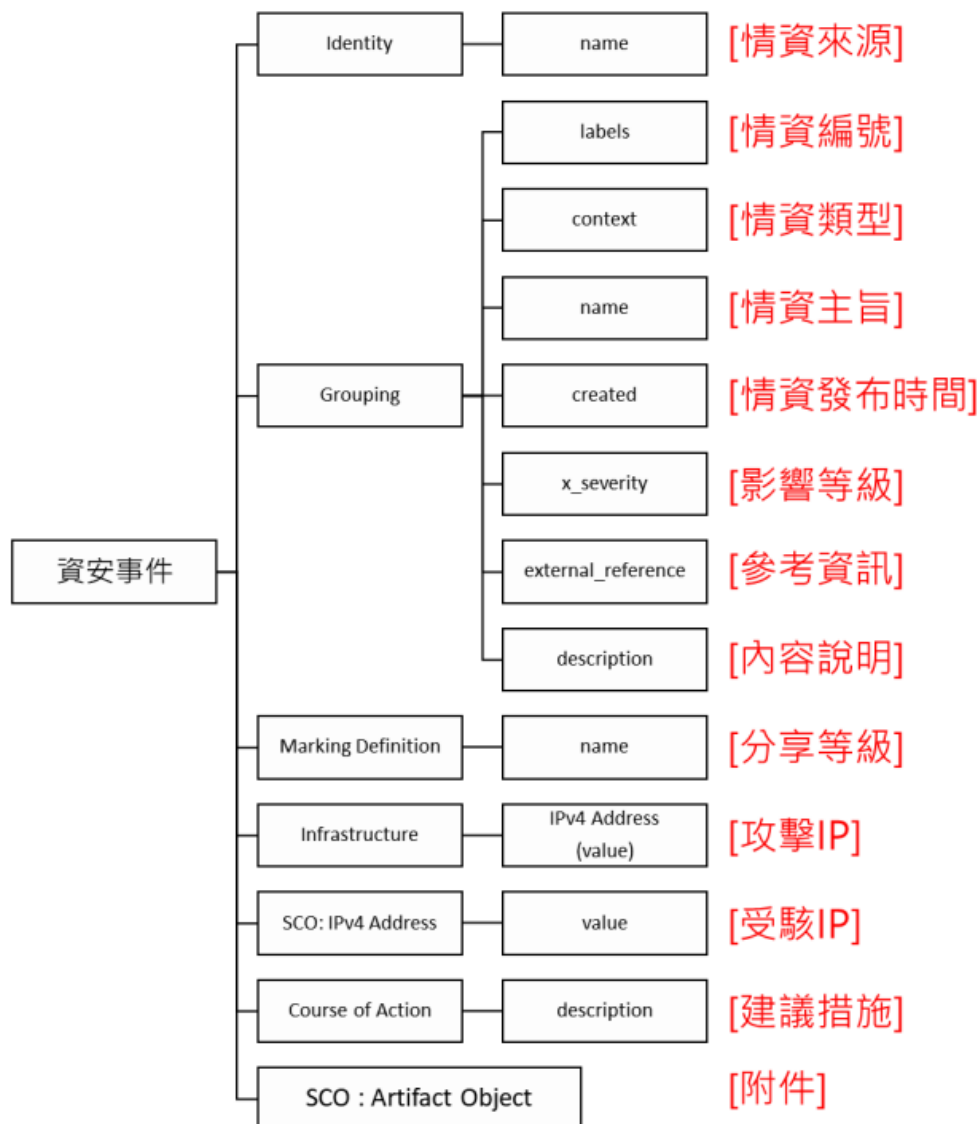


圖 73、N-ISAC 情資格式架構 1

資料來源：請參閱附錄-參考資料^{4.12}

N-ISAC 針對 4 種情資格式架構，依情資分類需求訂定不同驗證欄位，情資格式架構 1 的情資分類驗證欄位如圖 74 所示。

4.12 國家資通安全研究院. <https://www.nics.nat.gov.tw/.htm> (Jul. 03, 2023)

項次	欄位名稱	資安事件類型代碼									
		101	102	103	104	105	106	107	108	109	110
1	情資來源	系統自動帶入來源單位									
2	情資編號	系統自動帶入編號									
3	情資分類	101	102	103	104	105	106	107	108	109	110
4	情資主旨	必填欄位									
5	情資發布時間	必填欄位									
6	影響等級	限定為 4 級數字 { 1,2,3,4 }									
7	內容說明	必填欄位									
8	參考資訊	-									
9	分享等級	限定為 { red,amber,green,white }									
10	攻擊 IP			必填	必填	-	必填	-		-	
11	受駭 IP	至少 1 項	至少 1 項	-	-	必填	-	必填	至少 1 項	必填	至少 1 項
12	建議措施	必填欄位									
13	附件	-									
14	必要物件		Malware							Vulnerability	

圖 74、N-ISAC 情資格式架構 1 驗證欄位

資料來源：請參閱附錄-參考資料^{4.12}

(一)情資分類：以數字代碼來表示，如惡意內容：101，惡意程式：102，如圖 75 所示。

4.12 國家資通安全研究院. <https://www.nics.nat.gov.tw/.htm> (Jul. 03, 2023)

情資分類					
代碼	101	102	103	104	105
資安事件類型	惡意內容	惡意程式	資訊蒐集	入侵嘗試	入侵攻擊
代碼	106	107	108	109	110
影響等級					
影響等級		1	2	3	4
說明	弱點等級 (CVSS 3.0)	Low	Medium	High	Critical
	資安事件 影響等級	1級事件	2級事件	3級事件	4級事件
分享等級					
分享等級	Red	AMBER		GREEN	
說明	情資內容不應揭露 僅限參加者知悉	情資內容皆露範圍 僅限參與者組織內部		情資內容可揭露 予可明確界定之特定 群體	

圖 75、情資分類、影響等級、分享等級

資料來源：請參閱附錄-參考資料^{4.12}

(二)影響等級：內容限定為 4 級數字「1」、「2」、「3」、「4」，影響等級判定原則，4 Critical 4 級事件，如圖 75 所示。

(三)分享等級：以顏色來表示，如 Red 代表情資內容不應揭露，僅限參與者知悉。宜透過口頭說明或親自提供，不適合進行自動化情資分享，如圖 75 所示。

三、STIX 2.1 資安事件的範例

N-ISAC 使用 1 個物件 Identity 做為【情資來源】，本物件為必要情資欄位且不使用屬性 Description，當情資檔案傳入 N-ISAC 時，將由 N-ISAC 平臺自動更新檔案中物件 Identity 資訊。

情資來源範例如圖 76 所示，使用 STIX 物件是 identity。

4.12 國家資通安全研究院. <https://www.nics.nat.gov.tw/.htm> (Jul. 03, 2023)

```
{
  "name": "N-ISAC",
  "created": "2022-10-03T13:50:39.186Z",
  "modified": "2022-10-03T13:50:39.186Z",
  "spec_version": "2.1",
  "id": "identity--e735a647-5b7e-4b25-a2ce-3c605a010221",
  "type": "identity"
}
```

圖 76、情資來源範例

資料來源：請參閱附錄-參考資料^{4.12}

情資編號/類型/主旨/發布時間範例如圖 77 所示，使用 STIX 物件是 grouping。

```
{
  "name": "【情資主旨】xx公司所屬電子郵件帳戶疑似密碼洩漏",
  "description": "【內容說明】技服中心取得外部情資，發現xx公司所屬之電子郵件帳戶，其密碼資訊遭不明人士洩漏公開，疑似遭外洩之帳號密碼組合請參閱附件資訊。",
  "context": "【情資分類】107",
  "object_refs": [
    "ipv4-addr--654a8e6f-ee9d-4c7d-bc09-2ad681610e08",
    "ipv4-addr--5d6451e2-cd88-4563-aeed-0761627e5771",
    "course-of-action--baaede7-9392-45b6-be55-ca0a2b832ced",
    "artifact--7d115a49-e555-441e-a320-6e746c85d555",
    "identity--e735a647-5b7e-4b25-a2ce-3c605a010221"
  ],
  "created_by_ref": "【指向情資來源】identity--e735a647-5b7e-4b25-a2ce-3c605a010221",
  "labels": [
    "【情資編號】NISAC-107-202210-00000001"
  ],
  "created": "【情資發布時間】2022-10-03T13:50:38.936Z",
  "modified": "2022-10-03T13:50:38.936Z",
  "external_references": [
    {
      "source_name": "XSS防護手冊",
      "url": "https://www.cqisecurity.com/xss-faq.html"
    }
  ],
  "object_marking_refs": [
    "【指向分享等級】marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
  ],
  "spec_version": "2.1",
  "extensions": {
    "extension-definition--325ff21e-35e2-4c1a-9171-9c5d239711c4": {
      "x_severity": "【影響等級】2",
      "extension_type": "property-extension"
    }
  },
  "id": "grouping--e35029bc-8b34-41a0-929e-d2eda9b8d567",
  "type": "grouping"
}
```

圖 77、情資編號/類型/主旨/發布時間範例

資料來源：請參閱附錄-參考資料^{4.12}

4.12 國家資通安全研究院. <https://www.nics.nat.gov.tw/.htm> (Jul. 03, 2023)

分享等級範例圖 78 所示，使用 STIX 物件是 Marking Definition。

```
{  
  【分享等級】  
  "created": "2017-01-20T00:00:00.000Z",  
  "definition_type": "tlp",  
  "definition": {  
    "tlp": "amber"  
  },  
  "name": "TLP:AMBER",  
  "spec_version": "2.1",  
  "id": "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82",  
  "type": "marking-definition"  
},
```

圖 78、分享等級範例

資料來源：請參閱附錄-參考資料^{4.12}

建議措施與附件範例圖 79 所示，使用 STIX 物件是 Course of Action 及 Artifact。

```
{  
  "name": "建議措施",  
  "description": "【建議措施】通知相關單位或使用者，強化電子郵件密碼之保護措施，以免遭到未授權之存取或資料外洩",  
  "created": "2022-10-03T13:50:38.952Z",  
  "modified": "2022-10-03T13:50:38.952Z",  
  "spec_version": "2.1",  
  "id": "course-of-action--baaede7-9392-45b6-be55-ca0a2b832ced",  
  "type": "course-of-action"  
},  
  
{  
  【附件】  
  "mime_type": "application/x-zip-compressed",  
  "payload_bin": "UEsDBBQACQBJAAeSH1GgKAAAA==",  
  "spec_version": "2.1",  
  "id": "artifact--45a15ffe-f90f-48a1-a770-6fe69d180b94",  
  "type": "artifact"  
},
```

圖 79、建議措施與附件範例

資料來源：請參閱附錄-參考資料^{4.12}

四、STIX 格式限制及改善方式

本工作項目針對 AI-Native Security、in-X 子網 Network Slicing Security、IP Spoofing、DoS、Downgrade Attack 等資安威脅進行研

4.12 國家資通安全研究院. <https://www.nics.nat.gov.tw/.htm> (Jul. 03, 2023)

究分析，並對應至 N-ISAC 之 STIX 2.1 情資格式，研究發現這 5 類攻擊手法所產生之資安事件雖可對應至國家資通安全研究院公告之 N-ISAC 情資格式，惟資安事件的「攻擊 IP」與「受駭 IP」僅能呈現 IPv4 (IPv4 Address Object)，若攻擊或受駭 IP 為 IPv6 設備，則無法對應。有鑑於上述無法對應之問題，可能的解決方法有 2 種：

(一)新增 IPv6 Address Object，定義 IPv6 表示式：參考目前 N-ISAC 所提供 STIX 2.1 對受駭 IP 與攻擊 IP 之表達方式如圖 80 所示，建議可新增 IPv6 Address Object 如下，以定義 IPv6 表示式：

```
{  
  "value": "2001:0db8:85a3:0000:0000:8a2e:0370:7334",  
  "spec_version": 2.1,  
  "id": "ipv6-addr—xxx...",  
  "type": "ipv6-addr"  
}
```

惟新增 IPv6 Address Object 需考量現有 N-ISAC 對於欄位處理規格、長度、儲存、後續自動化處理等因素。

```
{
  "value": "【受駭IP】 123.123.123.123",
  "spec_version": "2.1",
  "id": "ipv4-addr--654a8e6f-ee9d-4c7d-bc09-2ad681610e08",
  "type": "ipv4-addr"
},
{
  "name": "Attack IP",
  "created": "2022-10-11T16:16:14.318Z",
  "modified": "2022-10-11T16:16:14.318Z",
  "spec_version": "2.1",
  "id": "infrastructure--c585dfca-e78e-4e75-9a17-d01fc02ef215",
  "type": "infrastructure"
},
{
  "value": "11.11.11.11",
  "spec_version": "2.1",
  "id": "ipv4-addr--c7f49c87-a394-4df8-aa35-34a9113a45c1",
  "type": "ipv4-addr"
},
{
  "relationship_type": "consists-of",
  "source_ref": "infrastructure--c585dfca-e78e-4e75-9a17-d01fc02ef215",
  "target_ref": "ipv4-addr--c7f49c87-a394-4df8-aa35-34a9113a45c1",
  "created": "2022-10-11T16:16:14.318Z",
  "modified": "2022-10-11T16:16:14.318Z",
  "spec_version": "2.1",
  "id": "relationship--529d8476-11ff-4be5-bc2b-7ef99b77980f",
  "type": "relationship"
},
}
```

圖 80、受駭 IP 與攻擊 IP 之 STIX 2.1 表達方式

資料來源：本計畫整理

(二)指定一特定 IPv4 位址，再將 IPv6 位址放置於附件表示：由於 IPv6 無法直接轉換以 IPv4 表達，因此可藉由指定一特定 IPv4 位址，例如：0.0.0.0，以表達此 IP 之位址為 IPv6，再將詳細之 IPv6 位址列於「附件」欄位表示。但此方式將不利於後續的自動化處理分析與分享。

第五節 6G 應用自動攻防與情資雛型系統情境實證先導評估

本分項規劃計畫的 6G 應用自動攻防驗證將在邊緣運算平臺上進行模擬 6G 環境的 AI-Native Security。隨著 AI 技術的快速發展應用，5G 已經開始深度結合 AI 以推進網路性能和功能。從 3GPP 和開放式無線接取網路聯盟 (Open Radio Access Network Alliance, O-RAN Alliance) 的動作可以明確看出這個發展趨勢。

首先，從 3GPP 的策略和發展來看，該組織已在其 R18 版本中確立了導入 AI 的共通框架。此外，還制定一套評估方法，讓 AI/ML 模型可以更有效地融合到無線介面 (Air Interface) 功能中。另外，O-RAN Alliance 在其制定的網路架構中，已經考慮了 AI 做為 RAN 架構中的重要元素，引入無線接取網路智慧控制器 (Radio Access Network Intelligent Controller, RIC) 的 AI 管理與控制功能，以集中管理 RAN 的 AI/ML 模型，基地臺可以根據即時情境利用模型做出最佳決策。從 3GPP 以及 O-RAN Alliance 的規格引入 AI 技術發展來看，可以歸納出 RAN 產業標準將會導入 AI/ML 成為標準的一部分。

未來 6G 可能採用更全面的 AI 整合策略，以含括 AI 最新技術發展，並內建 AI-Native 功能。而從網路軟體化、虛擬化以及 RAN 功能的分割 (Functional Splits)，可以預見未來 6G 環境中，每個 RAN 元件都可能具有自己的 AI 或 ML 模型，使得整個網路能夠自動調適與最佳化 QoS 與 SLA，如圖 81 所示的技術演進。

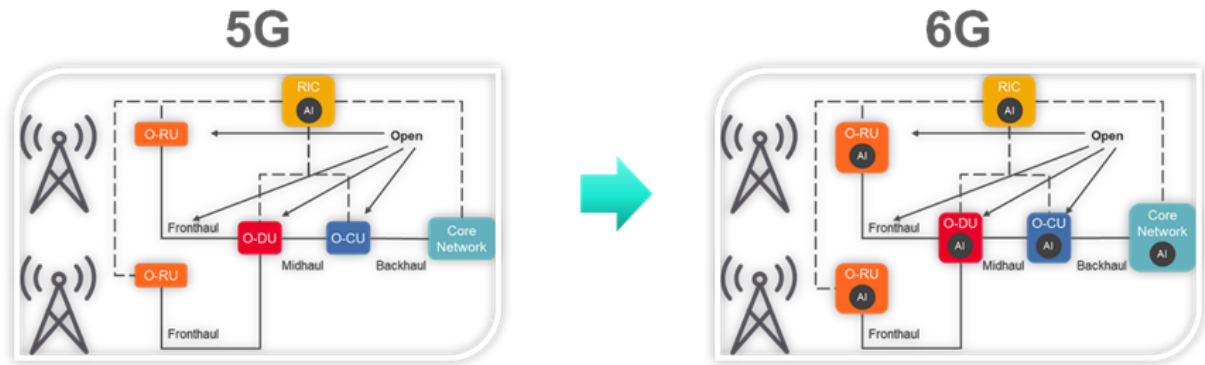


圖 81、5G 與 6G 導入 AI-Native 示意圖

資料來源：請參閱附錄-參考資料^{4.13}

在實證先導評估的規劃上，首先，將模擬 RAN 的 AI 功能，而此一 AI 功能將透過深度強化學習(Deep Reinforcement Learning, DRL)來進行無線資源分配(Radio Resource Allocation)管理，接著將對此一 AI 功能進行攻擊測試，包含傳統攻擊、AI 攻擊，以瞭解 AI 模型面臨資安威脅時可能遭受的衝擊。近來許多研究描述針對 RAN 中的 AI/ML 模型的攻擊，導致 AI/ML 解決方案輸出錯誤的預測，或做出錯誤的控制決策，從而導致性能下降，甚至更糟的情況是中斷。在傳統攻擊的部分，將會對其發動 DoS 或 IP Spoofing 攻擊；在 AI 攻擊的部分，將採用訊號擾動攻擊(Universal Perturbation Attack, UPA)、策略滲透攻擊(Policy Infiltrator Attack, PIA)等較為前瞻創新的攻擊手法來驗證 AI-Native Security，以觀測 RAN 遭受攻擊的結果，同時將收集與分析 UE 端量測數據，例如：數據速率(Target Rate)、發射功率(Power)、頻寬(Bandwidth)等。

一、實證目的

本計畫所規劃的 6G 應用自動攻防實證先導評估，主要目的為驗證 6G 無線資源配置 AI 模型功能遭受傳統攻擊(DoS 或 IP Spoofing)，以及 AI-Native Security 的可能攻擊方式、影響及防禦策略，可以強化

4.13 <https://www.techgoindu.com/2023/06/23/artificial-intelligence-in-5g-and-6g> (Jul. 03, 2023)

RAN 及其上服務安全的認識，有助於應對和適應快速變化的網路環境，提早模擬 6G 時代可能的資安威脅。此外，透過這項實測驗證，觀察 RAN 服務品質受到攻擊影響的程度與範圍，收集重要參考資料，作為調整防護策略的依據。這將強化防禦意識與能力，使未來面對日益複雜的網路攻擊手法時，作出適當的回應處置，提升網路安全防護能力。面對未來 6G 時代，此項自動攻防驗證將展現其重要價值，協助提早發展有效的威脅偵測技術與防禦策略。

二、與 ISO27001:2022 控制項目的對應

從實測結果來看，在傳統攻擊部分，由於 AI 模型並沒有抵擋攻擊的能力，因此對 AI 模型所運行的系統實施入侵偵測保護，諸如 IDS/IPS 等防護措施是必要的，而這些防護措施可以對應到 ISO27001:2022 的控制項 8.20 Networks security。而在 AI 攻防的部分，由於此次實證重心在 AI 攻擊的部分，因此並沒有提出防禦機制，且由於 AI 防禦仍然屬於非常前瞻的研究領域，相較於 DoS 等傳統攻擊已累積將近 30 年的研究，AI 攻擊的防禦技術目前仍在探索中，因而無法在此次提出防禦建議並對應至 ISO27001:2022 控制項。

三、測試方法

在環境建置的部分，利用 Open AI Cellular (OAIC)建置模擬 O-RAN 環境的測試平臺，本實證已初步完成平臺建置，在平臺上進行 UE 跟 BS 間通訊的模擬。BS 基地臺跟 UE 間的通訊分成 3 種類型，eMBB、MTC、URLLC，以 3 個切片模擬這 3 種不同資料傳輸特性。UE 個數有 40 個，BS 個數有 4 個，設定的方法與 UE 編號所對應的切片將在測試步驟小節中說明。實證會模擬針對 3 個切片實施 UPA 以及 PIA。

對抗性攻擊 AI 基礎資源分配，被認為是 AI 原生 O-RAN 功能中最嚴重的威脅之一。來自使用者設備的上行信號，是無線資源分配訓

練的來源，這些都可以被偽造的使用者設備或干擾信號輕易操縱，而且這些偽造的使用者設備可以輕易地使用軟體定義無線電設備建立。

以下說明在實測中所使用的 AI 模型以及攻擊的方法：

(一)DRL 無線資源分配 AI 模型

1. 代理(Agent)：在無線資源分配模型中，代理是學習和做出無線資源配置決策的主體。
2. 環境(Environment)：代理與之互動的外部環境。本模型的環境為 UE 與 BS 模擬。
3. 行動(Action)：代理可以在給定的狀態下採取的決策或動作。本模型的行動為 Downlink 功率選擇、子頻道。
4. 狀態(State)：描述環境當前情境的資訊。本模型的狀態為數據速率、發射功率、位置、佔用頻道。
5. 獎勵(Reward)：當代理採取某個行動後，環境會根據這個行動的好壞給予代理一定的回饋或獎勵。本模型的獎勵則是基地臺的吞吐量(Throughput，單位為 Mbps)等數值。
6. 策略(Policy)：一個從狀態映射到行動的函數。在 DRL 中，策略通常由神經網路(例如 CNN 或循環神經網路)表示，本 AI 模型使用開源的無線資源分配策略來進行實證。

(二)攻擊方法

1. 傳統攻擊

DoS & IP Spoofing：在這個模型中，使用 hping3 工具生成一個帶有虛假 IP 地址的 DoS 攻擊，如下所示：hping3 -a 192.168.0.10 192.168.0.100 -S -q -p 80，其中 192.168.0.10 到 192.168.0.100 是假 UE IP 地址。

2. AI 攻擊

攻擊方的目標是計算出敵對干擾，以使損失函數最大化。因此，資源分配可能會出現無法實現的解決方案或非最佳解

決方案，如此將降低 UE 端的通訊品質。攻擊方生成敵對的干擾樣本，表示為 $x_{adv} = x_t + \eta$ ，如所示。 η 是通過快速梯度符號方法、隨機干擾及動量迭代快速梯度符號方法幾種技術計算出來。接著，位置的敵對性模式被載入敵對訓練的輸入數據，以找到功率分配的模式。然後，攻擊者可以請求惡意 UE 廣播類似於所產生模式的虛假位置和訊號功率。

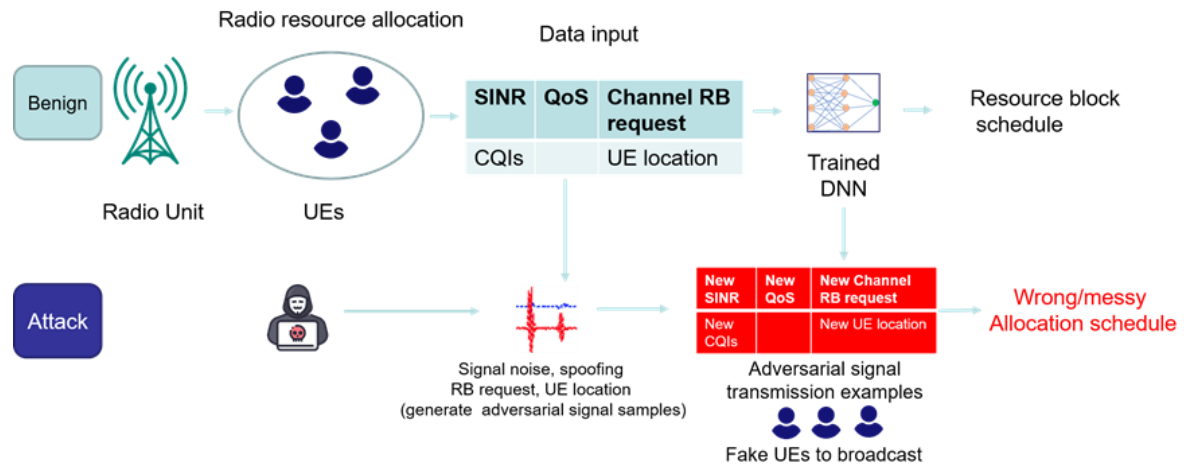


圖 82、多階段 ML 設計

資料來源：

本計畫實施 2 種攻擊類型，目標是訓練並建議 UE 的新干擾位置，誤導信號分類或誤導 DRL 政策方向。

1. UPA

這項技術根據損失函數的梯度來干擾輸入。在資源分配問題中，對手可以干擾通道狀態預測。此攻擊旨在干擾提取的 CSI 資料 H_K ：

$$\mathcal{H}_K^{adv} = \mathcal{H}_K + \epsilon \text{sign}(\nabla_{\mathcal{H}_K} \mathcal{L}_{RA})$$

其中 ϵ 是一個小的干擾幅度， $\nabla_{\mathcal{H}_K}$ 代表了相對於通道矩陣 $\mathcal{H}_K$ 的資源分配損失函數 $\mathcal{L}_{RA}$ 的梯度。

2. PIA

這項技術可以在考慮干擾幅度限制的情況下，優化對抗性干擾：

$$\mathcal{H}_K^{adv} = \Pi_C(\mathcal{H}_K + \alpha \text{sign}(\nabla_{\mathcal{H}_K} \mathcal{L}_{RA}))$$

其中 α 為步幅， Π_C 是將有效通道矩陣投影到可行集 C 上的運算子。

四、測試環境及架構

測試環境如圖 83，其中 AI 元件的部分採用 OAIC 開放原始碼(如圖 84 左側綠色及藍色 2 個方框內的軟體功能)模擬出無線電資源分配與管理(Radio Resource Allocation and Management)功能，此部分的功能將會以外掛 Plugin 的方式與服務管理與編排(Service Management and Orchestration, SMO)介接。RAN 與 UE 採用 srsRAN 軟體模擬。本測試平臺規格可利用現有硬體設備進行部署，透過模擬軟體進行攻防實測驗證。而傳統攻擊架構如圖 85 所示。



圖 83、測試環境

資料來源：本計畫整理

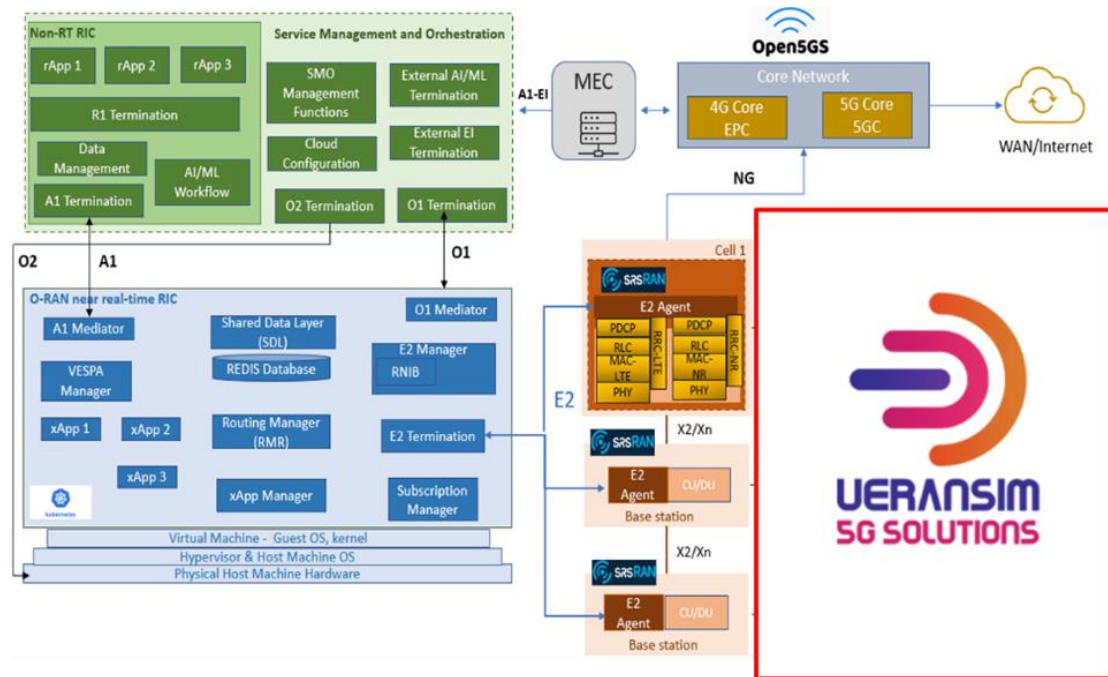


圖 84、實證先導評估使用的 5G 環境模擬軟體

資料來源：本計畫整理

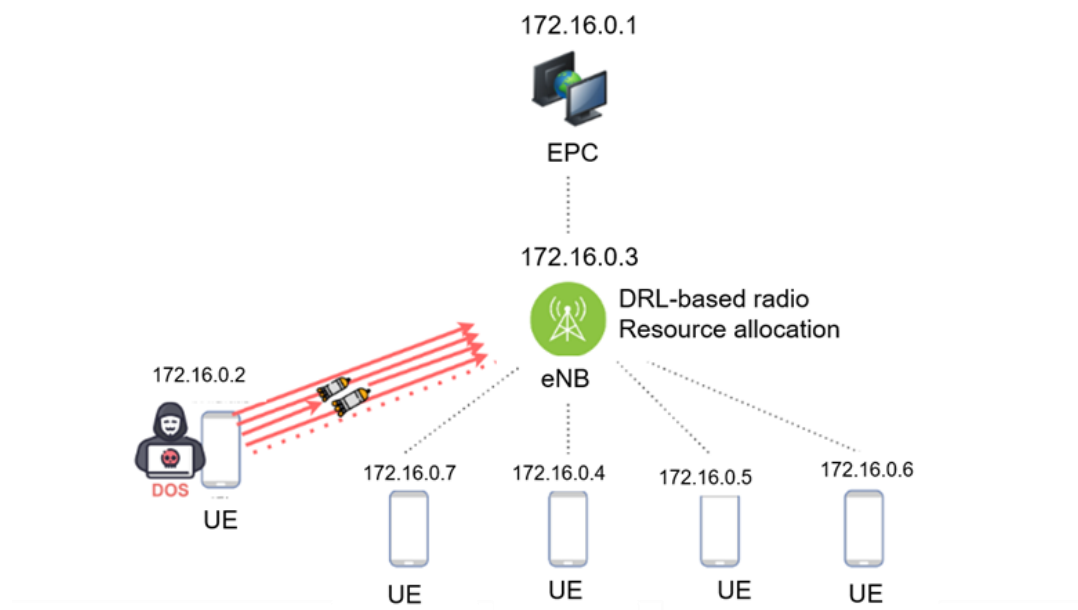


圖 85、傳統 DoS 攻擊的測試架構

資料來源：本計畫整理

AI 攻擊測試架構如圖 86 所示，本實證採用 OAIC 軟體模擬 O-RAN 環境，gNB 的部分使用 srsRAN 模擬，每個 gNB 會設定 3 個切

片，對應到 5G KPI 的 3 項特性，設定方法於測試步驟小節中說明。UE 的部分，因為本實證規劃 40 臺終端設備，且要模擬終端設備上不同的使用狀況，例如：串流應用、IoT 應用情境等，因此使用 srsRAN 模擬 UE，並且設定不同的流量特性，將 UE 跟 gNB 傳輸流量收集成資料集進行對抗性攻擊模擬測試，如圖 86 右側所示。40 臺 UE 設方法於測試步驟小節中說明。

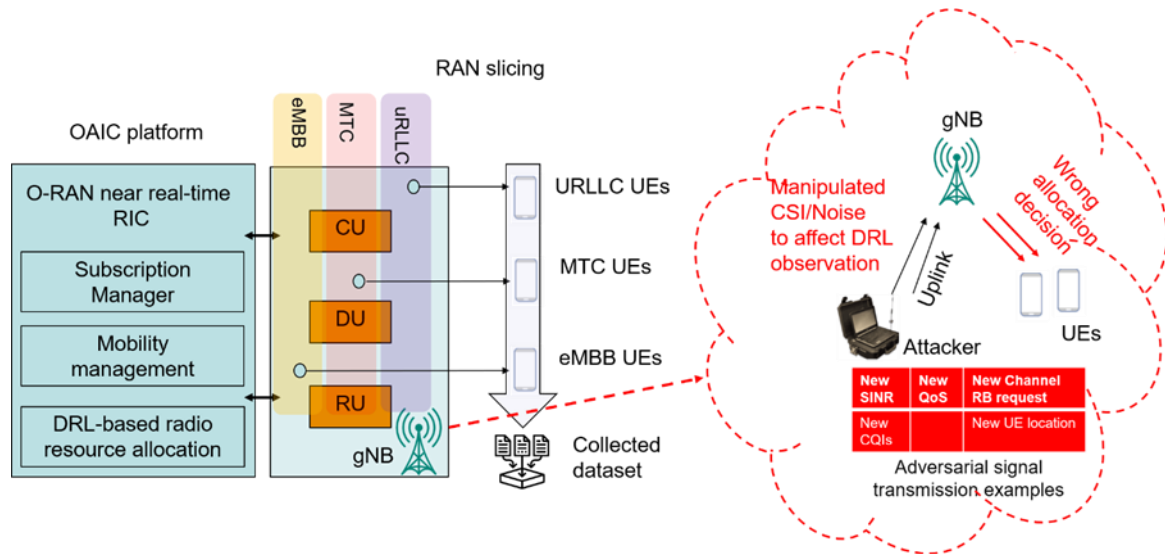


圖 86、AI 攻擊測試架構

資料來源：本計畫整理

五、使用之軟硬體

表 33、實證軟硬體說明

名稱	OAIC Controller (模擬 UE/BS/Attacker/AI 模型)
硬體規格	CPU：Intel i7-6700@3.4GHz DRAM：32GB HDD：256GB
作業系統	Ubuntu 20.04 LTS
程式軟體	Python 3.5+ Cloudpickle 1.4.1 Numpy 1.19 Scipy 1.4.1 Tensorflow 2.3 tf-probability 0.7
網路介面	RTL8111/8168/8411 gigabit Ethernet controller
其它項目	以下為模擬 UE 跟 BS 資料傳輸的規格 UE 個數 40 UE ID 分配給不同的通訊流量類別： eMBB UEs：2, 5, 8, 12, 15, 18, 22, 25, 28, 32, 35, 38 MTC UEs：3, 6, 9, 13, 16, 19, 23, 26, 29, 33, 36, 39 uRLLC UEs：1, 4, 7, 10, 11, 14, 17, 20, 21, 24, 27, 30, 31, 34, 37, 40 Uplink 1.02GHz Downlink 0.94 GHz 通道頻寬 3MHz 無線頻率配置設定 近(Close)：UEs uniformly distributed within 20 m of each BS 中(Medium)：UEs uniformly distributed within 50 m of each BS 遠(Far)：UEs uniformly distributed within 100 m of each BS 模擬基地臺覆蓋 0.11km ² 切片 eMBB, MTC, uRLLC 排程策略 (PF), (WF), (RR)



	行動管理：Pedestrian user mobility with time-varying path loss and channel conditions
備註	(無)
名稱	DRL 測試機器
硬體規格	• Intel® Core™ i7-10700F 2.9GHz • 16 GB RAM Nvidia GTX 1660
作業系統	Ubuntu 20.04 LTS
程式軟體	• Python 3.5+ • Cloudpickle 1.4.1 • Numpy 1.19 • Scipy 1.4.1 • Tensorflow 2.3 tf-probability 0.7

資料來源：本計畫整理

六、測試步驟

(一)環境建置

利用 OAIC 建置模擬 O-RAN 環境的測試平臺，包含架設近即時無線接取網路智慧控制器(Near-Real-Time Radio Access Network Intelligent Controller, Near-RT RIC)、將 E2 介面整合至 RAN、設定 RAN 和 xApps 之間的服務模型，以及在測試平臺上測試控制 RAN 的 AI 模型。OAIC 模擬 O-RAN 軟體，使用 Git 工具將軟體下載至測試機器，詳細的安裝指令可以參考 OAIC 網站^{4.14}，由於 O-RAN 環境安裝繁瑣且須具備相關工具使用的預備知識，因此以下僅列出關鍵步驟設定，完整的軟體安裝設定流程請參考 OAIC 網站^{4.15}，主要步驟包含：

1. 安裝 srsRAN 4G/5G 軟體堆疊，從原始程式碼安裝的腳本如下：

```
cd srsRAN-e2
mkdir build
export SRS=`realpath .`
cd build
cmake ../ -DCMAKE_BUILD_TYPE=RelWithDebInfo \
-
DRIC_GENERATED_E2AP_BINDING_DIR=${SRS}/e2_
bindings/E2AP-v01.01 \
-
DRIC_GENERATED_E2SM_KPM_BINDING_DIR=${S
RS}/e2_bindings/E2SM-KPM \
```

4.14 GitHub. openaicellular/oaic. Retrieved from <https://github.com/openaicellular/oaic.git>

4.15 OAIC.(2022). Retrieved from <https://openaicellular.github.io/oaic/quickstart.html>

```
DRIC_GENERATED_E2SM_GNB_NRT_BINDING_DIR  
=${SRS}/e2_bindings/E2SM-GNB-NRT  
make -j`nproc`  
sudo make install  
sudo ldconfig  
srsran_install_configs.sh user --force  
cd ../../
```

2. 在容器部署 RIC 元件，包含 E2 管理器、E2 終結點、訂閱管理器、路由管理等服務。OAIC 已將 Near-RT RIC 元件封裝至容器內，並已叢集(Cluster)的方式透過 Kubernetes 來部署這些元件，部署 Kubernetes 叢集的腳本程式在前述下載程式碼的目錄 RIC-Deployment/tools/k8s/bin 中。當 Kubernetes 叢集部署完畢後，最後一步即是部署 Near-RT RIC 功能，如下指令：

```
cd RIC-Deployment/bin  
sudo./deploy-ric-platform-  
f ../RECIPE_EXAMPLE/PLATFORM/example_recipe_oran_e_release_modified_e2.yaml
```

3. 部署非即時 RIC 元件，在部署之前，執行如下指令取得該元件程式碼^{4.16}、^{4.17}。
4. 執行相關的腳本檔案，完畢後執行如下指令部署非即時 RIC 元件^{4.18}：

```
cd ~/nonrttric/bin
```

4.16 GitHub. openaicellular/nonrttric. Retrieved from <https://github.com/openaicellular/nonrttric.git>

4.17 GitHub. openaicellular/main-file-repo. Retrieved from <https://github.com/openaicellular/main-file-repo.git>

4.18 O-RAN Non-Real Time RIC Installation Guide. Retrieved from <https://openaicellular.github.io/oaic/nonrttric.html>

```
sudo./deploy-nonrtric-  
f ../RECIPE_EXAMPLE/NONRTRIC/example_recipe.yam  
l
```

(二)測試資料收集

測試資料收集使用 KPIMON xApp，所記錄的 log 內容會存在 /var/log/kpimon/kpimon.log 中，可供後續統計分析研究用。本實證所使用 UE 基地臺流量測試資料集整理如表 34。

表 34、測試資料集

檔案大小	1.49 GB
資料分類	slice_mixed, slice_traffic
資料錄製時間長短	480s
資料收集回合數	17
基地臺資料特徵個數	4 (time,nof_ue,dl_brat,ul_brat)
UE 端資料特徵個數	21 (time, cc, pci, earfcn, rsrp, pl, cfo, dl_mcs, dl_snr, dl_turbo, dl_brat, dl_bler, ul_ta, ul_mcs, ul_buff, ul_brat, ul_bler, rf_o, rf_u, rf_l, is_attached)

資料來源：本計畫整理

(三)傳統攻擊測試步驟

對執行 AI 網路元件的機器發動傳統 DoS 攻擊，以 hping3 工具程式對 port 80 發出大量高速的 icmp 封包，指令如下：

```
hping3 -a 192.168.0.10 192.168.0.100 -S -q -p 80
```

(四)AI 攻擊測試步驟

1. 執行無線資源分配 AI 模型

無線資源分配 AI 模型為基於 DRL 的 AI 模型，可根據 UE 的數據速率、發射功率、位置、佔用頻道等，透過強化學習計算出對 UE 最佳的下行功率。本實證計畫以此來模擬未來 6G 環境下，AI 網路元件會為使用者設定基地臺最佳的

無線資源分配。由於本實證計畫的重點在於探索智慧化基地臺可能的弱點，並試圖對基地臺發動攻擊，因此在 AI 網路元件的部分，採用開源已訓練好的 DRL 模型進行無線資源分配模擬^{4.19}。

AI 模型在 ml_models 目錄下，已根據 3 種不同的 5G 網路流量 eMBB、MTC 及 uRLLC 訓練出在這些情境下配置無線資源的最佳策略。這 3 種情境所對應的 DRL 強化學習模型分別在如下目錄：embb_policy、mtc_policy、urllc_policy。這些模式是使用 Tensorflow DL 框架，在使用前必須先安裝 Tensorflow 框架，以下列指令分別載入 3 個模型的參數：

```
drl_agents=[tf.saved_model.load(embb_policy_filename),  
             tf.saved_model.load(mtc_policy_filename),  
             tf.saved_model.load(urllc_policy_filename)]
```

欲使用這些模型，則可將 O-RAN 的 DU 單元所收到來自於 UE 的無線資源配置要求作為輸入參數，呼叫 DRL 模型的 action 函數取得最佳配置，如下所示：

```
action = drl_agents[i].action(time_step)
```

其中，time_step 即為 DU 單元所收到的 UE 配置要求，而 action 則為 DRL 模型的輸出下行功率。

2. 執行訊號擾動對抗性攻擊

執行訊號擾動對抗性攻擊 python 程式碼 FGSM_Adversarial_Attack.py，這種攻擊方式採用快速梯度標記法(Fast Gradient Sign Method, FGSM)生成對抗示例來攻擊資源配置模型，其工作流程如表 35。FGSM 攻擊方法藉

4.19 GitHub. wineslab/colosseum-oran-commag-dataset. Retrieved from <https://github.com/wineslab/colosseum-oran-commag-dataset>

由添加縮放後的梯度符號來擾亂良性輸入資料，目的在於最大化損失並生成能欺騙 ML 模型的對抗輸入。

表 35、AI 攻擊測試步驟-訊號擾動對抗性攻擊工作流程表

執行項目	執行訊號擾動對抗性攻擊
執行流程	1. 從 CSI 矩陣 H 中取出 UE n 的原始 RBG 特徵。 2. 計算資源配置損失函數 L_{RA} 對輸入 RBG 特徵的梯度： $\nabla H \times L_{RA}$。 3. 確定梯度的符號：$\text{sign}(\nabla H \times L_{RA})$。 4. 用一個小的常數 epsilon (ϵ) 對梯度符號進行縮放：$\epsilon \cdot \text{sign}(\nabla H \times L_{RA})$。 5. 將縮放後的梯度加到原始 RBG 特徵上以獲得對抗樣本： $H_{adv\_x} = H_x + \epsilon \cdot \text{sign}(\nabla H \times L_{RA})$。 6. 檢查對抗示例 H_{adv_x} 是否會導致資源配置模型做出錯誤的決策並最大化損失 L_{RA}。 7. 如果損失沒有被最大化，調整 epsilon (ϵ) 值並重新生成對抗樣本。 8. 重複步驟 2 至 7，直到損失 L_{RA} 被最大化並且模型做出錯誤的資源配置決策。 9. 最終擾亂的 RBG 特徵 H_{adv_x} 構成使用 FGSM 攻擊方法針對資源配置模型生成的對抗樣本。

資料來源：本計畫整理

3. 執行策略滲透對抗性攻擊

執行策略滲透對抗性攻擊 python 程式碼 Policy_Infiltrator.py，其工作流程如表 36。PIA 藉由迭代地添加小的符號梯度雜訊來最大化損失，並生成能誤導資源分配決策的對抗輸入。

表 36、AI 攻擊測試步驟-策略滲透對抗性攻擊工作流程表

執行項目	執行策略滲透對抗性攻擊
執行流程	1. 將對抗輸入 δx 初始化為良性輸入 X，並設定擾動大小 ε 與最大迭代次數 N。 2. 通過資源分配模型 M 對良性輸入 X 進行推論，計算基準預測。 3. 進行 N 次迭代。 4. 計算損失函數 $\nabla XJ(\delta x, \text{基準預測})$ 的梯度。 5. 通過添加經 ε 縮放的梯度符號,更新對抗輸入 δx。 6. 將 δx 裁剪保持在 X 的 ε 範圍內,以約束擾動大小。 7. 通過模型 M 對對抗輸入 δx 進行推理,獲得入侵預測。 8. 如果入侵預測與基準預測不同，或擾動大小超過 ε，跳出迴圈。 9. 否則，重複步驟 4 至 7。 10. 在 N 次迭代或提前停止後，最終擾亂的輸入 δx 構成使用 PIA 生成的對抗示例。 11. 在推理時使用對抗輸入 δx 而不是真實輸入 X 來攻擊資源分配模型 M。

資料來源：本計畫整理

七、測試數據及測試結果之探討

(一)傳統攻擊的測試結果

測試 UE 個數為 20，發動 DoS 攻擊前，每個 UE 的平均 datarate 為 1.3Mbps，如圖 87：

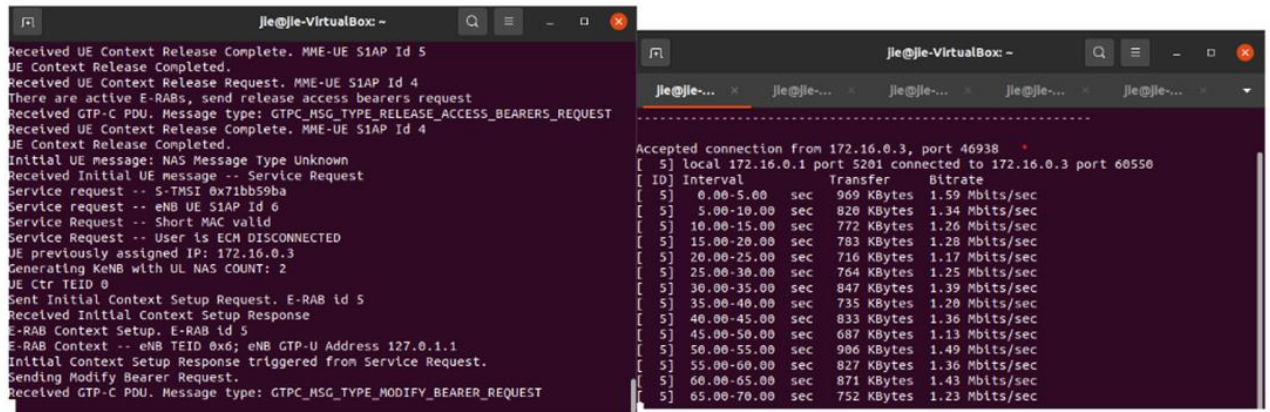


圖 87、傳統測試攻擊結果

資料來源：本計畫整理

發動 DoS 攻擊後，4G 基地臺(Evolved Node B, eNB)立刻超過傳輸負載量，UE 端的平均 datarate 降至 0 Mbps，如圖 88。攻擊從第 200 秒開始。連線中斷顯示基於 AI 的無線電資源分配大幅受到傳統 DoS 和 IP 偽冒攻擊影響。

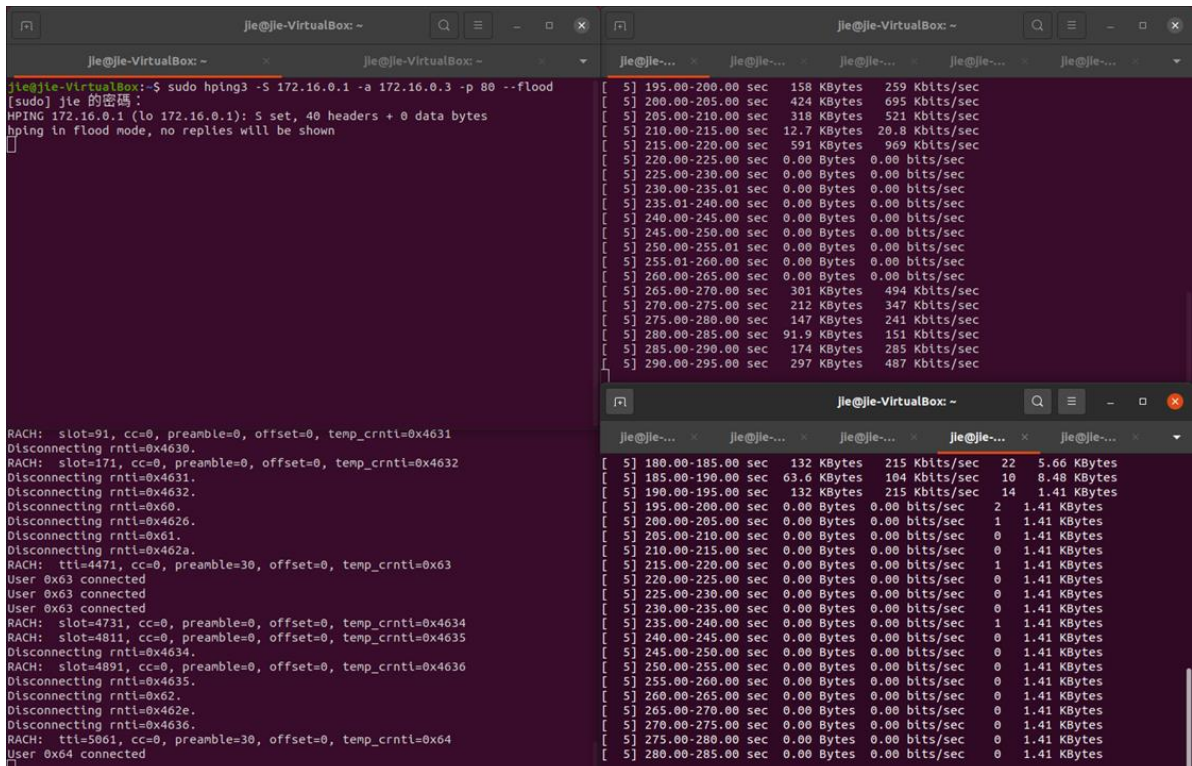


圖 88、發動 DoS 攻擊 UE 端的平均 datarate

資料來源：本計畫整理

(二)AI 攻擊的測試結果

實驗測試數據如表 37。

表 37、AI 攻擊實測結果

切片	無攻擊 (Mbps)	訊號擾動攻擊 (UPA) (Mbps)	策略滲透攻 擊(PIA) (Mbps)	降級比例 (%)	
				UPA	PIA
eMBB	3.39	2.99	2.36	12	29
MTC	0.14	0.12	0.12	26	26
uRLLC	0.05	0.04	0.03	20	40

資料來源：本計畫整理

從測試結果發現，UE 所需的延遲越低，在攻擊後受到的負面影響越大。這是因為對抗性攻擊造成了資源分配請求的長時間延遲，導致當超過時間限制後，封包被迫丟棄。在像 uRLLC 這樣的低延遲服務中，這種超時會造成很大的負面影響，因為通訊中的較長延遲可能導致潛在事故，例如在高速公路上行駛的高速車輛。此外，PIA 在降低使用者設備的 datarate 方面比 UPA 方法更有效，這是因為 PIA 直接影響到 DRL 學習策略，而 UPA 需要時間藉由 DRL 觀察過程產生效果。

第六節 小結

本計畫團隊研究觀察 6G 與 5G 在網路威脅方面的差異，從最新的文獻分析整理出 4 項不同點，分別是(1)網路威脅的規模可能擴大且複雜性變高、(2)邊緣運算與網路切片技術的成熟，未來 6G 網路曝露風險的攻擊面(Attack Surface)變得更廣，如何達成各層級(Layer-wise)、全面向(從 UE 端、RAN、Edge 端到核網)的安全防護將更具挑戰、(3)AI/ML 技術被利用進行攻擊，由於 AI/ML 模型輸出的隨機性，將使得威脅的來源、模式、影響範圍難以分析預測、(4)隨著新的身分驗證技術、加密技術發展，以及量子運算可能破解加密系統的隱憂，隱私與資料保護的討論程度將在未來 6G 時代更加被熱烈探討與研究，如何掌握相關關鍵技術、標準制定，並在國際上佔有一席之地，不僅攸關國內 6G 資安產業發展，更是屬於國安議題因而影響深遠。本章接著針對未來 6G 資安技術的發展列出 6G 資安需求，代表未來 6G 資安技術解決方案所需具備的特點，包含(1)需能保護資料的機密性與完整性、(2)使用操作及設定的自動化、(3)身分驗證技術產生的用戶隱私需獲得保護、(4)需有輕量化解決方案以應對各式連網裝置、(5)需更即時快速地回應資安威脅、(6)對能源消耗要求低。在滲透測試規範研析的部分，本章整理 NIST 出版關於 5G 資安的測試規範，以及 OWASP 出版的測試規範等相關內容，同時也列出國內 5G IoT 場域資安防護評估指引，以呈現國內外在定義滲透測試規範的現況。

針對 6G 網路 5 種攻擊，分別為 AI-Native Security、in-X 子網 Network Slicing Security、IP Spoofing、DoS、Downgrade Attack 等資安威脅進行研究，了解攻擊手法、防禦及緩解措施。對於可以支援 6G 網路威脅的情資格式，本章介紹國外的 STIX v2.1 情資格式標準，以及我國在 STIX 情資格式標準上所定義的「N-ISAC 情資格式說明」。綜合所研析的內容，在實證先導評估部分，選擇對 DoS、AI-Native

Security 進行資安威脅模擬，以探索先進無線網路中的 AI 網路元件遭受 DoS、AI 攻擊所受到的衝擊影響。

一、滲透測試規範研析

在滲透測試規範的研析，以 5G 核網滲透測試進行說明，介紹了 NIST 所發布的參考測試架構，其中測試節點在參考架構中的安排，可以讓測試節點對架構中的無線、有線設備，其上執行的服務，以及安全功能進行端點至端點的驗證測試，因此可以在此參考架構中執行 5G 核網滲透測試等關鍵項目，包含 NFV 測試、SDN 測試、身分驗證和授權測試、互連安全測試等項目。在現階段 6G 標準尚未制定完成之前，藉由 5G 核網滲透測試架構研析，可做為規劃未來 6G 滲透測試的參考。另外，台灣資通產業標準協會提出 IoT 場域資安防護評估指引，該指引目的是為推動國內 5G 垂直應用發展，以建立適用於國內 IoT 場域的資安評估機制，本節透過列表的方式整理出 IoT 場域滲透測試規範所定義的 17 項滲透測試項目。由於臺灣 IoT 場域資安防護評估指引在制定過程中，亦審酌國外 OWASP 規範，因此針對 OWASP 規範進行說明，介紹主要測試項目，包含身分驗證測試、Session 管理測試、資料驗證測試等做為比較參考。

二、6G 應用服務層之偵防工具化可行性評估

針對 6G 網路 5 種攻擊，分別為 AI-Native Security、in-X 子網 Network Slicing Security、IP Spoofing、DoS、Downgrade Attack 等資安威脅進行研析，了解攻擊手法、防禦及緩解措施，最後對於這 5 項威脅的偵防工具化評估提出如下建議：

(一)AI-Native Security

建議的偵防工具 McAfee MVISION，為綜合性網路安全平臺，結合 AI 和 ML 等先進技術，為組織提供主動保護、威脅情報和統一管理。MVISION 提供廣泛的安全功能，包括端點安全、雲端安全、資料保護以及威脅偵測和回應，並提供資料遺失防護(Data

Leakage Prevention, DLP)、加密和使用者行為分析等高級功能，以確保敏感資訊受到保護，使組織能夠增強其安全態勢並自動化事件回應。

(二) In-X 子網 Network Slicing Security

建議的偵防工具 FortiGuard，是一種商業工具，可用於檢測和減輕網路切片攻擊。FortiGuard 網路切片安全使用 ML 和異常檢測等多種技術來識別惡意活動。

(三) IP Spoofing

建議的偵防工具 NIDS (如 Snort 或 Suricata) 可以配置為檢測表明 IP 欺騙的網路流量模式。如果在短時間內觀察到多個子網上來自單個源 IP 地址的流量，則可能表明存在欺騙。

(四) DoS

建議的偵防工具 Radware DefensePro，是一種基於硬體的解決方案，用於檢測和緩解各種類型的 DoS 攻擊，包括流量攻擊、應用層攻擊和 SSL 攻擊，使用行為分析和實時簽名創建來提供保護。

(五) Downgrade Attack

建議的偵防工具 OSSEC，是一個開源 IDS，可用於檢測各種攻擊，包括 Downgrade Attack。OSSEC 可用於監控網路流量是否存在惡意活動，還可以用於監控系統日誌是否存在可疑活動。

另一個建議的偵防工具 Snort，是一個可用於檢測 Downgrade Attack 的開源 IDS。Snort 與 OSSEC 類似，但 Snort 提供了更廣泛的特性和功能。

三、可支援 6G 網路威脅資訊結構

資安事件的情資分享與訊息通報是整體資安防護能夠產生效果的重要關鍵，因此研析了可以進行網路威脅情資通報與交換的標準化格式 STIX 2.1，STIX 格式可以被應用於網路威脅分析的描述，定義網路威脅特徵的分類。當資安事件發生時，運用 STIX 格式來交換情

資，有利於建立共通的情資系統，使網路威脅資訊分享、事件管理、事件回應等動作皆有一致的格式定義，對於情資系統自動化，建立聯防體系將產生相當關鍵的效果。本章也研析 N-ISAC 根據 STIX 2.1 標準所制定的「N-ISAC 情資格式說明」，並列出以 STIX 2.1 描述資安事件的範例，以及其格式限制與改善方式。藉由本工作項目之研析，已找出目前 N-ISAC 之情資格式之不足，並提供可能的解決方法，以提升政府情資分享架構在 6G 環境之可用性。

四、6G 應用自動攻防與情資雛型系統情境實證先導評估

在 6G 應用自動攻防與情資雛型系統情境實證先導評估的部分，選擇所研析 5 項威脅的第 1 項 AI-Native Security 進行實證。從本章第一節研析 6G 與 5G 在網路威脅方面的 4 項差異中，可以發現 AI/ML 技術內建在未來網路基礎建設中可能面臨的資安威脅將難以預測防範。隨著高效能運算(High Performance Computing, HPC)的成熟發展帶來超級電腦整體算力的大幅提升，所訓練出 AI/ML 模型也更加強大，諸如 ChatGPT 等 AI 的商業應用，已出現在每天的日常生活中。若這些 AI/ML 模型、演算法、訓練資料、訓練流程遭到駭客惡意攻擊，有可能帶來難以估計的損失與災難性後果。從第三節研析的 AI-Native Security 可判斷未來 6G 基礎建設中，將會應用 AI 做網路的部署、配置及管理。基於此，本實證先導評估嘗試在 RAN 中模擬 AI 模型做資源配置，並分別以傳統攻擊，例如：DoS，以及 AI 攻擊，例如：對抗式攻擊(本實證所採用 UPA、PIA 攻擊演算法皆屬於此範疇)，分別對 AI 資源配置模型進行攻擊，以比較 2 種攻擊的衝擊影響。實證結果顯示：

- (一)AI 模型的網管功能對傳統資安攻擊方式並無顯著抵抗能力，
仍需有對應阻斷式攻擊等資安防護機制。

- (二)AI 對抗式攻擊，對 AI 網路資源配置演算法可造成顯著破壞，Throughput 降低約在 10%至 40%不等，視網路資源配置策略與攻擊手法不同，而有不同的降級比例以下。
- (三)測試發現 UE 所需的延遲越低，對抗性攻擊造成資源分配請求的長時間延遲，導致當超過時間限制後，封包被迫丟棄，在攻擊後受到的負面影響越大。
- (四)對於傳統攻擊的防禦建議，佈署 AI 模型的機器面對傳統 DoS 攻擊方式並無顯著抵抗能力，因此仍需藉由設置入侵偵測、防火牆等實體設備，來阻擋傳統 DoS 惡意攻擊。對於 AI 攻擊的防禦上，應投入開發和部署針對對抗性攻擊的防禦機制，例如偵測和過濾對抗性輸入，以增強 AI 模型的強健性。另外，應建立 AI 模型輸入資料的檢查機制，蒐集影響模型的樣本進行分析與重新標示，當發現 AI 模型效能異常時，可擴大訓練資料集以涵蓋這些異常樣本，並重新訓練新的模型使能抵擋對抗性攻擊。
- (五)本實證項目係由本團隊與陽明交大、中正大學的網路資安實驗室合作產出，成果應用將視產業需求進行推廣。

第五章 6G 資安產業研析與防護實證應用驗測先導評估

未來在 6G 行動網路的環境下，預期可達到無縫立體的全域覆蓋連接，於此基礎下萬物互聯將會有更多的人、物、服務連上網路，也就意謂這更多資料，甚至是隱私個資會在網上到處傳遞，所以對於資訊安全的防護也更就越顯得重要。

首先第一節將從全球 Pre-6G 資安技術最新演進現況觀察，各國政府針對 6G 使用案例以及使用技術，提出包含供應鏈或資安議題的任何缺點，並引用全球行動通訊系統協會(Groupe Speciale Mobile Association, GSMA)制定的網路設備安全保證方案(Network Equipment Security Assurance Scheme, NESAS)作為檢測驗證 Pre-6G 系統架構安全之測試流程、實驗室認證與系統評估等機制，是全球流通最廣的通訊資安認證體系，預期 3GPP 會員廠商們將在 NESAS 的基礎下，持續探索相關的安全技術推動因素，發展 6G 系統需要確保全面性 IoT、異質雲端網路、設備、子網路和應用服務安全技術。

在第二節中銜接國際 6G 資安現況，探討我國 6G 資安服務框架與推動機制，由於網通設備「白牌化」商機是我國資通訊產業的優勢，應可鼓勵國內業者與國際市場上主導開放架構布建的系統整合商，建立硬軟優勢互補的合作關係，打入國際電信商的供應鏈，並建議政策支持投入 6G 次世代通訊前瞻布局，重視資安防護機制，研擬 5G 延伸到 6G 建立相關資安標準規範，衍生需求議題發生可能性較高，發展群聚科技生態系的特性，累積充足研析資料，推進產業 6G 發展方向，形成以智慧化高可靠度為主軸的新興產業生態系。

在第三節將 6G 資安產業研析的初步結論，設計資安防護應用驗測實證評估方法，由 2G、3G 發展出來的 GSM 系統之單向認證機制仍存在缺陷，從而讓假基地臺有機可趁，源於運用身分驗證或訪問控制機制是 6G 安全期待已久的功能，本節提出「假核網+基地臺誘騙

用戶攻擊」、以及「假用戶對核網的攻擊」等 2 大類型 4 種資安攻擊情境，分述假基地臺及假用戶連線的情境與危害，規劃測試環境、方法與步驟，測試攻擊發生的影響程度，雖然目前有關 6G 無線通訊標準的資訊還很少，本團隊仍針對現行正在探討演進中的 6G 無線網路基礎架構元件的特性，實作避免使用者認證資訊產生洩漏風險，導致阻斷使用者應用無線網路服務，並防止假冒網路基地臺或攻擊者誘騙網路用者，產生隱私資訊洩漏，提升系統可信賴性與資料隱私安全。

技術實證結果對應 6G 關鍵性技術指標可靠性(Reliability)與安全和隱私(Security and privacy)，4 項資安風險議題分別對應 ISO 27001：2022 控制措施「A.5.30 營運持續之 ICT 備妥性」、「A.8.9 組態管理」、「A.8.16 監視活動」導入建議防護作法，驗證緩解方案可行性，除做為發展 6G 網路軟硬體資安技術建議，在國內廠商參與國際組織討論會議時，回饋國內 Pre-6G 相關資安技術的前期研究與測試結果，形成國內外技術同步的正向循環。

最後在第四節參酌國際發展通訊資安趨勢及本計畫研究技術主題，藉助國內台灣雲端物聯網產業協會已成立物聯網資安 SIG，分別於 5/17、8/29、9/19 及 10/5 完成 4 場技術交流座談會，會議中邀請包括專網維運商、系統整合、設備供應商、資安和研究機構等超過 90 家廠商(含因防疫線上參加)，取得不同參與者建議通訊世代安全主題面向。

第一節 全球 Pre-6G 資安技術發展趨勢

當前 ITU-R 定義的 5G 系統頻寬、用戶體驗網路流速及裝置連接密度分別是 10-20 Gbps、100 Mbps 及 100 萬/平方公里，而對應 6G 指標將可能分別達到 1 Tbps、10-100 Gbps 及 1000 萬/平方公里，成長性約 10-100 倍，6G 將成為全自動化全域覆蓋 IoT 爆發的起點。在具有巨量入網設備以及超高頻寬的情況下，攻擊行為會更易於隱蔽，將進一步增加傳統攻擊行為的檢測難度。

雖然 5G 已經對無線接入網路的影響很大，但 6G 也將面臨許多新挑戰，主要是由頻率的大幅增加推動，這將促進所有地方對天線的需求，以及開發 THz 頻率的商業收發器，於此同時無線傳輸將利用一些全新的 RAN 方法來增強網路頻寬和減少延遲，例如：MIMO 技術來提高頻譜效率，結合陸海空鏈路連接、超密集無線電接入點部署，以及多項關鍵技術與 6G 融合如圖 89，包括 AI、大數據分析和邊緣雲端運算等形成 HetNet 異質網路整合與協作環境。

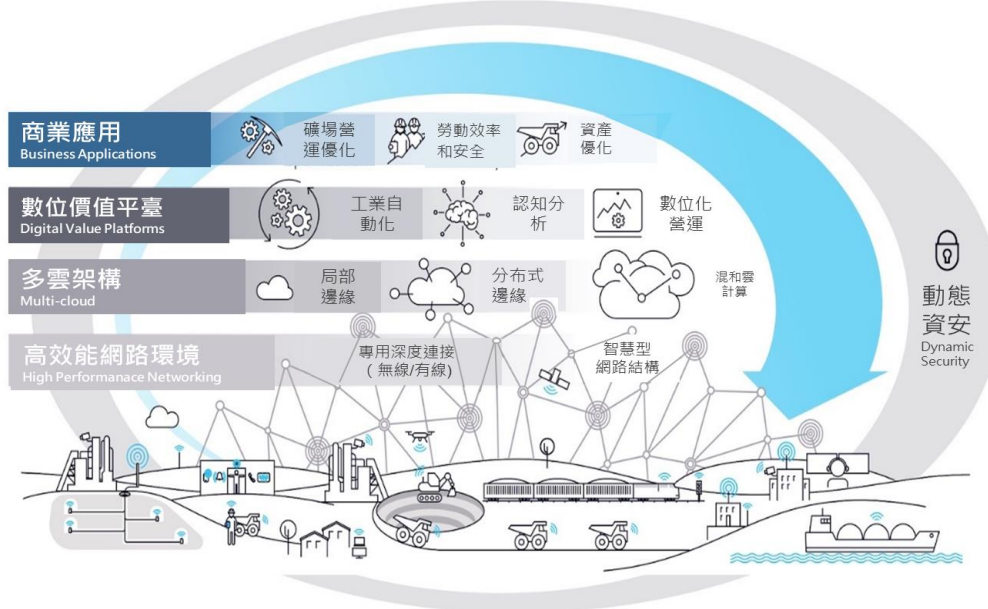


圖 89、6G 網路環境高度整合 AI、大數據分析與邊緣運算

資料來源：請參閱附錄-參考資料^{5.1}

5.1 6G Flagship

一、GSMA 發展 NESAS

針對 6G 系統架構的安全議題，美國聯邦通訊委員會(Federal Communications Commission, FCC) 根據美利堅合眾國眾議院(United States House of Representatives, U.S. House)通過的「未來網路法(Future Uses of Technology Upholding Reliable and Enhanced Networks Act, FUTURE Networks Act)」等相關法案，針對 6G 使用案例以及使用技術，提出包含供應鏈或資安議題的任何缺點。

美國與歐盟成立貿易與科技理事會(EU-US Trade and Technology Council, EU-US TTC)的第 4 工作組-資通技術安全與競爭力(Working Group 4: ICTS security & competitiveness)亦將 6G 資安納入其主要的議題之一。不論是美國與歐盟都以全球行動通訊系統協會(Groupe Speciale Mobile Association, GSMA)制定的網路設備安全保證方案(Network Equipment Security Assurance Scheme, NESAS)作為驗證 Pre-6G 系統架構安全的基礎。以下便針對 NESAS 做進一步說明：

(一)NESAS

6G 網路將會帶動整個上下游供應鏈的發展，會以大量不同設備供應商加入 6G 產業中，因此對於供應鏈、產品設備風險的議題當中，GSMA 提出針對網路元件之 NESAS，適用於電信設備生命週期的安全保障。簡單來說，5G 技術主要依循 3GPP 技術標準制定，設備製造商可依循 3GPP 所制定之資安評估準則(Security Assurance Specification, SCAS)，設計其產品符合基本安全要求，GSMA 則針對支援 3GPP 定義功能網路產品的供應商構建 NESAS 安全認證框架，以提升行動產業的安全層級如圖 90 所示。

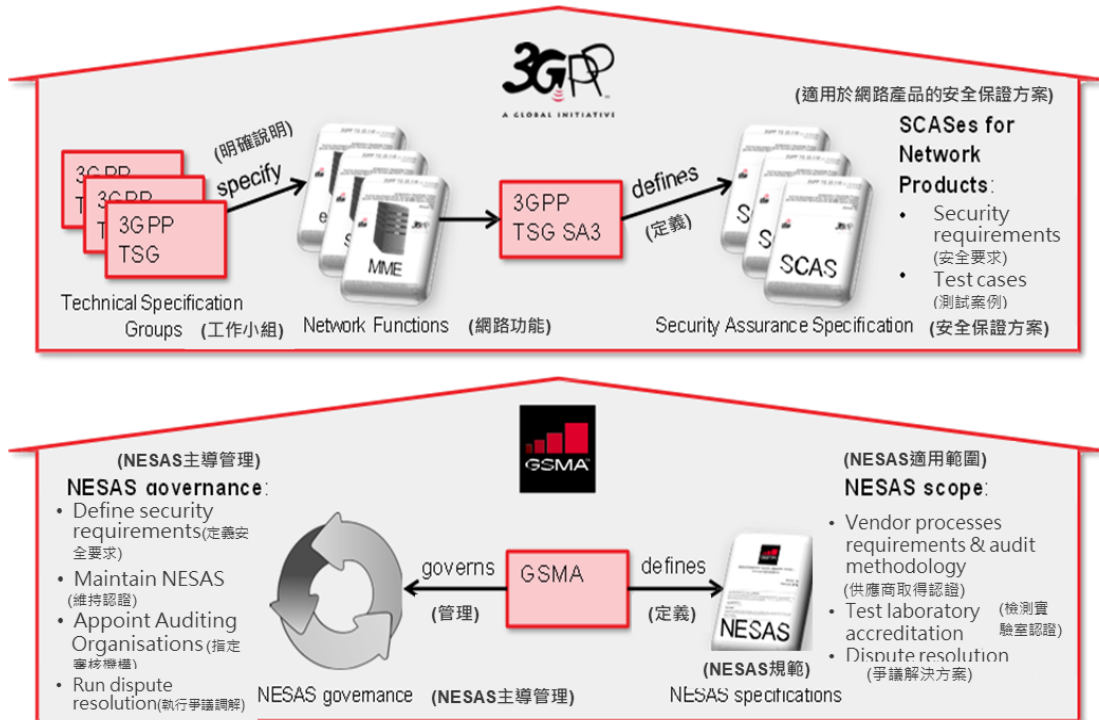


圖 90、NESAS 宗旨

資料來源：請參閱附錄-參考資料^{5.2}

第 1 階段為針對產品開發及生命週期管理流程的評估著重於安全保證方法流程，期望電信設備製造商可透過認證之第三方實驗室，取得各元件之安全認證，此方法可做為未來電信事業採購設備時，對安全性的認定標準。第 2 階段是製造商須將網路設備產品提交給 3GPP 定義是否合格，且須透過 ISO/IEC 17025 認證的 NESAS 安全檢測實驗室，進行實質效益的網路產品安全測試評估，其內容包含：測試程序、文件體系、流程維護等。網路設備安全檢測實驗室可以由製造商自行建立，也可以是由外部的獨立第三方擔任，每一家實驗室都經過 ISO/IEC 17025 認證機構的檢驗，檢試實驗室最後將記錄評估結果並撰寫報告，之後再提供給製造商，由製造商自行決定是否將結果對外公開如圖 91 所示。

5.2 GSMA. <https://www.gsma.com/security/network-equipment-security-assurance-scheme/>

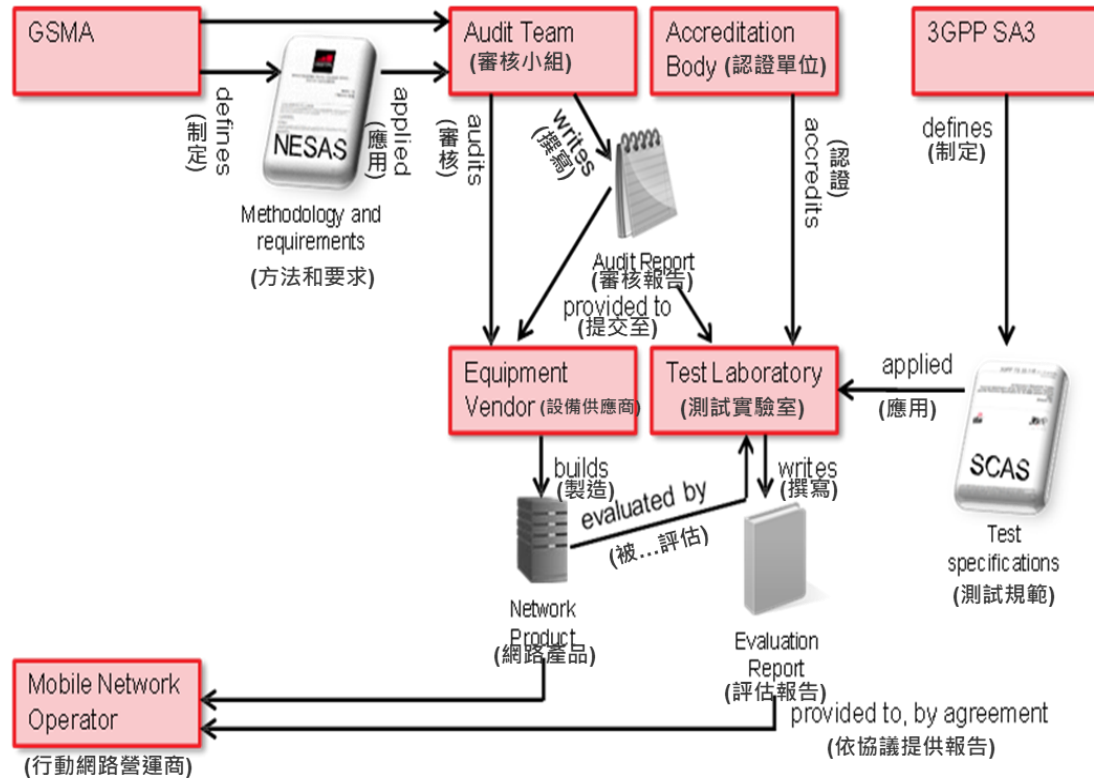


圖 91、NESAS 流程概述

資料來源：請參閱附錄-參考資料^{5.2}

GSMA 管理、制定並定期修訂整個 NESAS 規範，這項規範總體概述如圖 92，由左至右包含了安全測試實驗室認證、設備製造商的開發與產品生命週期認證、網路設備安全性測試評估：

1. 安全測試實驗室認證：GAMS 發展 FS.14 文件，制定的實驗室認證流程和要求，GSMA 對測試實驗室進行認證，只有通過認證的測試實驗室才能夠對網路設備進行安全評估。
2. 設備製造商的開發與產品生命週期之認證：依據 GSMA 發展 FS.15 和 FS.16 文件，由 GSMA 指定的獨立的驗證方執行，並輸出驗證報告。
3. 網路設備之安全性測試評估：安全測試實驗室依據 3GPP SCAS 規範對網路設備進行安全測試，對產品開發和生命週期進行安全評估。

5.2 GSMA. <https://www.gsma.com/security/network-equipment-security-assurance-scheme/>

週期管理流程是否真正應用到所測試的網路設備進行檢測，
向電信運營商提供網路設備的安全評估報告。

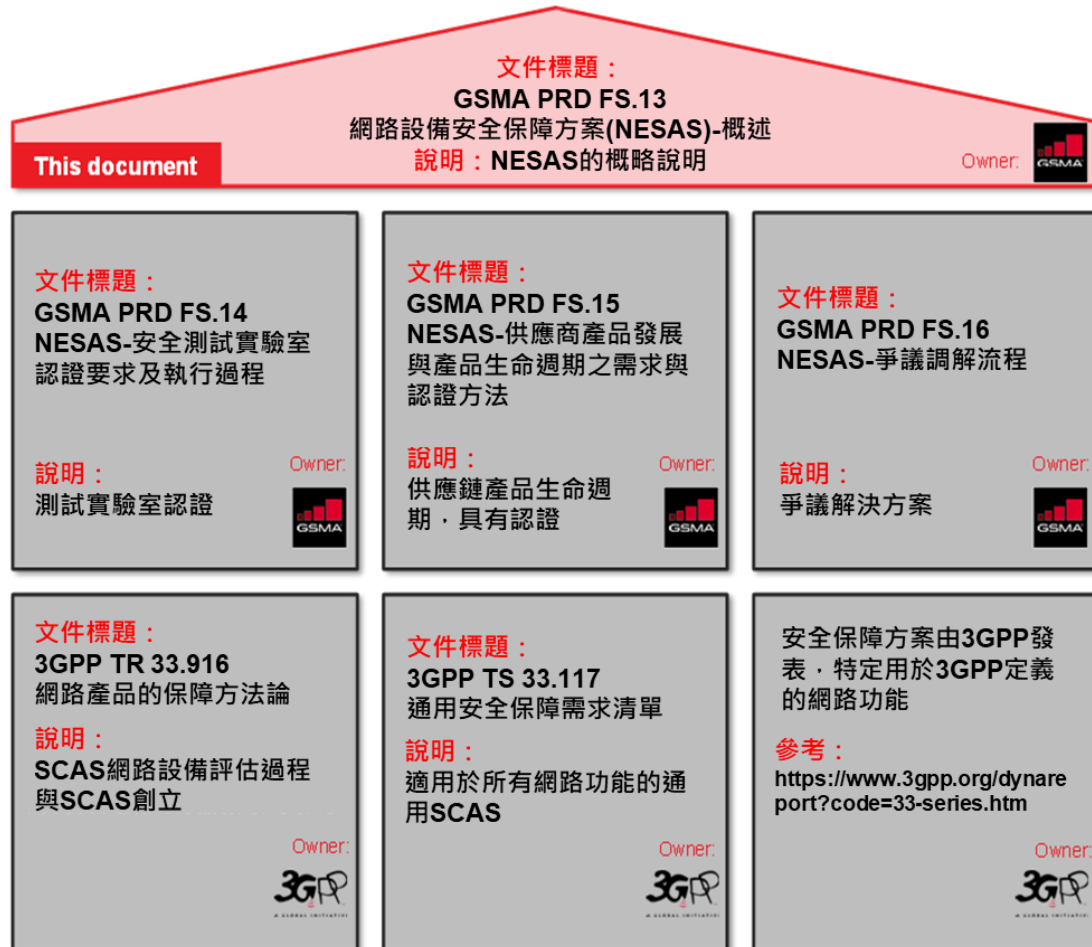


圖 92、NESAS 測試框架

資料來源：請參閱附錄-參考資料^{5.2}

而為了確保 3GPP 定義的各個網路元件的安全性，3GPP 展開安全保障及評估方法研究工作，成果彙整於 3GPP 網路產品安全保障方法研究(TR 33.805-Study on security assurance methodology for 3GPP network products)，網路產品安全評估方法論以目前最廣泛對 IT 產品進行安全評估的 CC 準則(Common Criteria；安全評估共通準則，ISO/IEC 15408)，分析其對 3GPP 網路產品的適用性，結論指出 CC 中評估不同的等級(EAL2 到 EAL4)刻畫安全評估的實施

5.2 GSMA. <https://www.gsma.com/security/network-equipment-security-assurance-scheme/>

程度和安全保障的不同的均衡點；而 3GPP 網路產品的安全評估範疇、評估深度是比較確定的，所以不需要 CC 那樣的評估等級，亦不需要 CC 的證書許可流程，因此，TR 33.805 所建議的方法論是藉用 CC 的一些方法論，製定 SCAS 安全要求和測試案例。

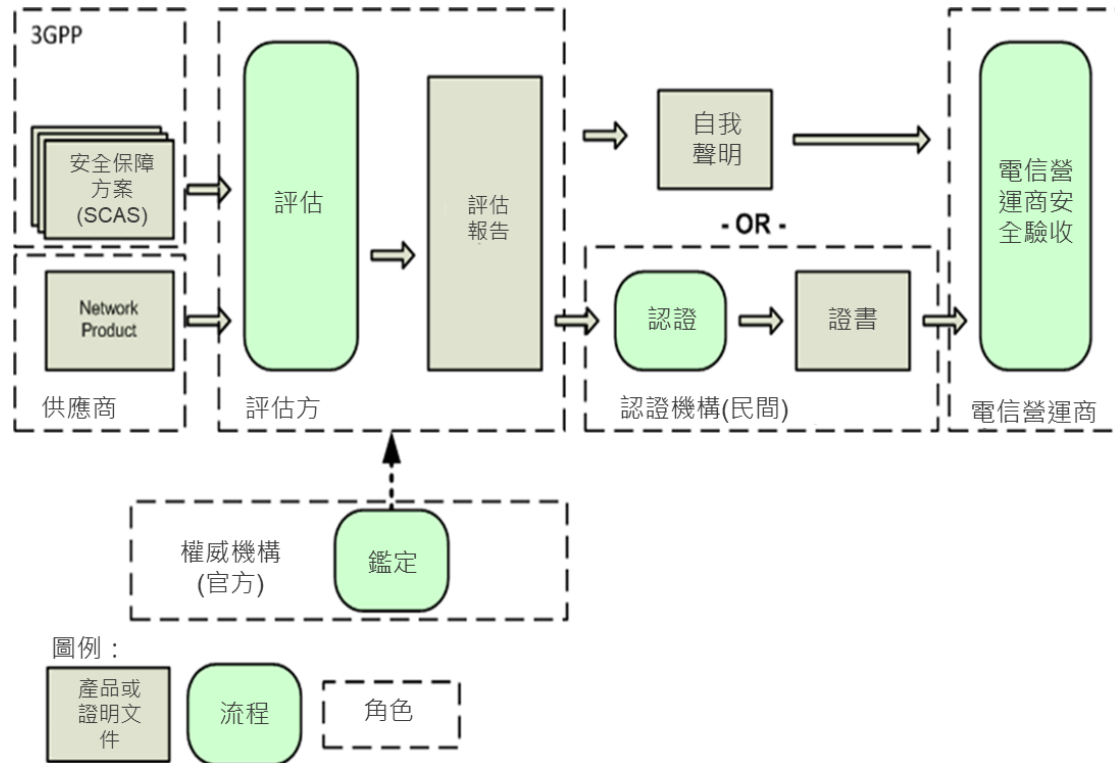


圖 93、SECAM 檢測流程

資料來源：請參閱附錄-參考資料^{5.3}

圖 93 即是 3GPP SCAS 建議之安全認證流程圖：左上由 3GPP 制定網路設備評估所使用的規格，廠商將網路產品提交給評估方，評估方需要由權威機構認可，以達到評估方的公信力，在 GSMA 的體系裡面，是由 ILAC 成員基 ISO 10725 來對一些具備條件的測試實驗室進行資格認證授權的，在我國則是由財團法人全國認證基金會(Taiwan Accreditation Foundatio, TAF)以 ISO 10725 條件進行資格認證授權，以利後續爭取國際相互承認之基礎；評估方基於 3GPP 的規範來進行評估，產生檢測評估報告，透過檢測評估報告，網路

設備廠商可以自聲明自己的產品通過了安全評估，也可以由一些權威認證方來頒發證書，說明廠商的安全具備 3GPP 所要求的安全性，最終電信運營商基於廠商的自聲明或權威認證，來作為廠商產滿足安全需求的參考依據。

針對 gNB 資安風險議題，未來在生產製造的過程中將會依據 SCAS 進行合規檢測，並由資安實驗室針對設備的弱點進行規範檢測及防駭漏洞檢測等 2 階段測試如圖 94。

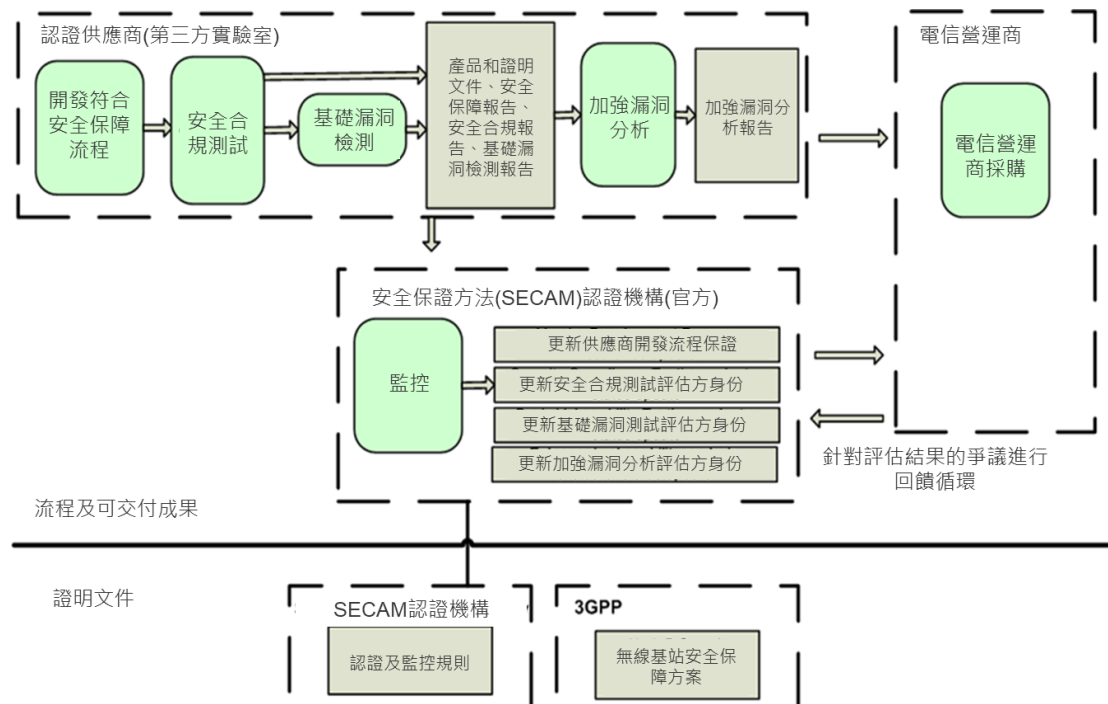


圖 94、5G 資安檢測流程

資料來源：請參閱附錄-參考資料^{5.4}

在弱點進行規範檢測部分，如：管理流量保護，對管理面的流量進行機密性和完整性保護，測試案例包括：所有的網路元件不接收未經保護的管理面流量；而防駭漏洞檢測則是類似滲透測試的作法，如：連接埠掃描，要求所有非網路業務需求的連接埠都應關閉，測試方式包括對網路設備的所有外部連接埠進行掃描。

5.4 3GPP TS 33.511

3GPP 創建 5G 的 SCAS，GSMA 則制定認證流程、產品開發過程的安全性審核，以及測試實驗室資質相關的 NESAS，確保落實 5G 網路安全，針對通訊安全測試評估的部分，NESAS 引用 3GPP 制定的 SCAS TS33 系列規範，包含 5G NSA eNB 基站與核網網路元件、5G SA gNB 基站、核網網路元件與通用性資安等標準項目，制定認證流程、產品開發過程的安全性審核，以及測試實驗室資格，為電信營運商和供應鏈廠商提供容易落地實施的安全保證，同時為產業確定一個通用的基準安全等級如圖 95。

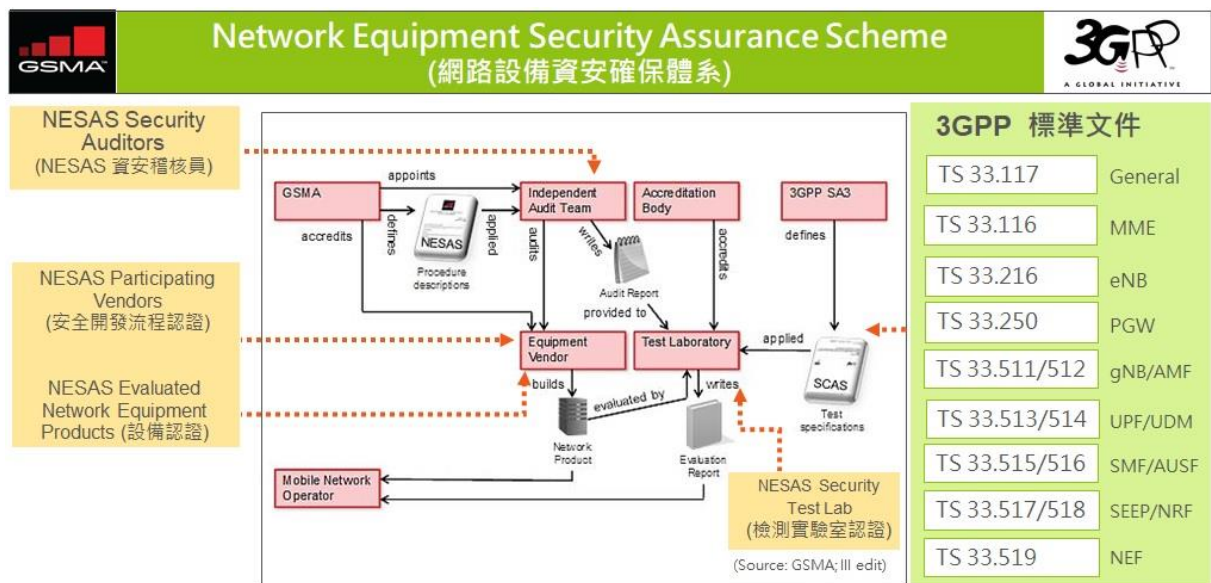


圖 95、NESAS 資安認證範圍

資料來源：請參閱附錄-參考資料^{5.2}

NESAS 資安認證範圍透過制定業界認同的安全基礎，為設備廠商和營運商提供安全保證的技術參考，對於設備供應商來說，NESAS 將有助於降低由於各國和地區的管制要求差異以及營運商的需求差異所導致的安全需求的碎片化，提供一個可以證明自身產品與能力符合國際標準的平臺；對於電信營運商來說，NESAS 提

5.2 GSMA. <https://www.gsma.com/security/network-equipment-security-assurance-scheme/>

供衡量廠商是否落實安全要求的可行方法，形成完整通訊產業安全防護網。

(二)NESAS 評價與分析

NESAS 對於行動產業相關業者、監管機構和廣大終端用戶具有重大價值。由於有 NESAS 體系，網路設備所達到的安全確保等級具可測量性、可視性、可比較性，幫助行動網路營運商確定各個廠商的網路設備是否符合行動網路營運的資安要求。對於廠商來說，NESAS 提供一個平臺，以彰顯廠商的實現/保持良好安全標準的能力。

推動大部分廠商提供確保產品開發和維護流程的安全承諾。這對電信營運商在選擇廠商時是很有益處的，因為它增加廠商可信度和電信營運商做決定的信心。另一方面，也鼓勵和促進廠商加強產品的安全性，並且從設計之初就將安全融入到產品之中，在設備廠商界形成一個良好的安全產品文化。

我國可承接第三方檢測業務之 5G 通訊資安檢測實驗室有 3 家，分別是：耀睿科技股份有限公司、財團法人電信技術中心、財團法人資訊工業策進會，目前 3 家皆通過 TAF 認證為 ISO 17025 實驗室，尚未向 GSMA 申請成為 NESAS 安全檢測實驗室，已可依據通訊設備廠商或系統建置廠商需求，提供 3GPP SCAS 測項檢測服務，並提供測試結果報告，擴散資安技術落地 5G 垂直應用場域，打造 5G 企業專網安全性與信賴度。

由具備資格認可的檢測實驗室執行網路設備評估，可以讓電信營運商在部署設備之前，就能夠確定該設備的安全等級。此外，NESAS 啟用高效成熟的認證模式，提供通用且確保基準安全級別，適用於所有客戶和市場安全要求，也為系統建置廠商、電信營運商、相關監管機構和國家主管部門，減少大量安全性測試的負擔，進而

節省成本、降低開銷及提高效率，最終會體現在網路設備的價格降低，創造利潤並逐步實現全域覆蓋的網路環境。

二、6G 安全性議題與隱私保護

依據 3GPP 今(2023)年 6 月 13 日至 16 日於臺北舉辦 3GPP SA R19 標準研討會中第 3 工作群組-安全性(SA3 Working Group - Security, SA3 WG)的討論與規劃，參與大廠認為 SCAS 的議題屬於檢測技術與其他資安議題不同，需要單獨舉辦標準會議討論 SCAS 相關議題，如圖 96 所示。

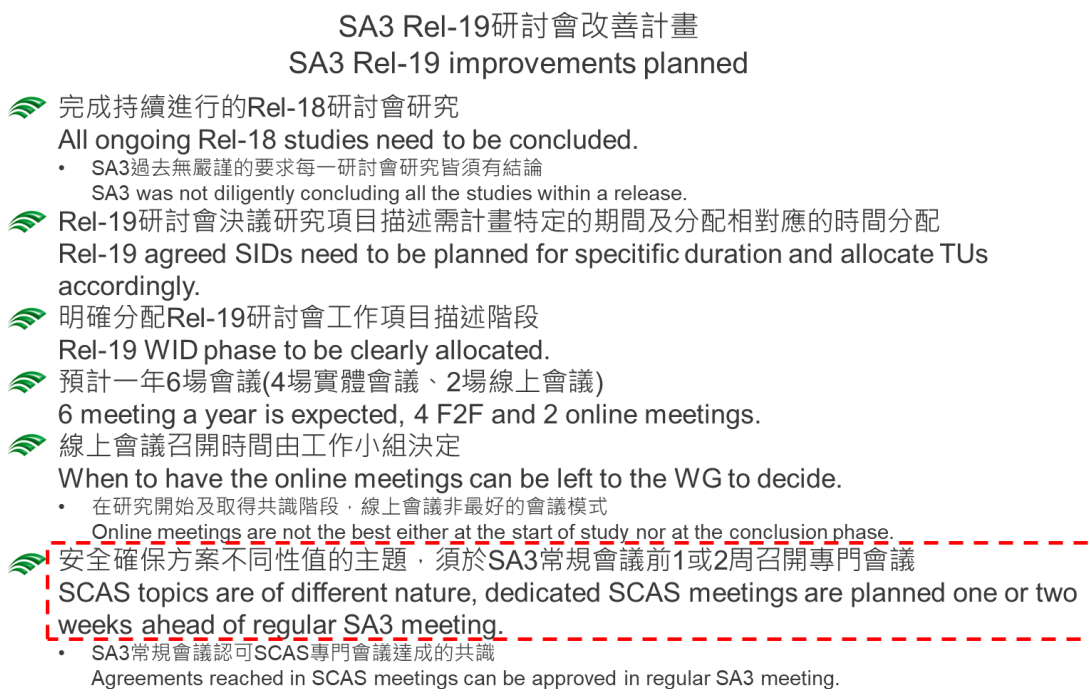


圖 96、3GPP 第 3 工作群組-安全性(SA3 WG)的工作規劃

資料來源：請參閱附錄-參考資料^{5.5}

依據 3GPP RAN R19 標準研討會如圖 97，Pre-6G 與資安議題相關技術如下：

啟用 AI 與 ML 的無線介面(AI/ML Air Interface)、環境物聯網(Ambient IoT)、移動性增強(Mobility Enhancement)、非地面網路演進(NTN Evolution)、擴展實境演進(XR Evolution)、啟用 AI 與 ML

5.5 3GPP SWS-230074, SA Release-19 workshop

的次世代無線接取網路(AI/ML NG-RAN)、自我組織網路(Self-Organizing Network, SON)/路測工作最小化(Minimization of Drive Test, MDT)、定位技術增強(Positioning Enhancement)、側鏈技術演進(Side-Link (SL) Evolution)、側鏈中繼技術演進(SL Relay Evolution)以及接取層安全性增強(Access Stratum (AS) Security Enhancement)。

- 人工智慧/機器學習空中介面
AI/ML Air Interface
- 多輸入多輸出演進
MIMO Evolution
- 雙工演進
Duplex Evolution
- 環境物聯網
Ambient IoT
- 增強網路能源儲存
Network Energy Saving Enhancements
- 增強傳輸性
Mobility Enhancements
- 非地面網路演進
NTN Evolution
- 擴展實境演進
XR Evolution
- AI/ML 的次世代無線接取網路
AI/ML for NG-RAN
- 自我組織網路/路測工作最小化
SON/MDT
- 增進無線通道模型演進(附加範圍如ISAC)
Channel Modeling(& possibly
Additional aspects e.g. for ISAC) for
Future evolution
- 額外由RAN1領導的專門主題
Additional RAN1-led Candidate Topics
 - 低功耗喚醒機制/喚醒接收器
LP-WUS/WUR
 - 增強多載波
Multi-carrier Enhancements
 - 增強覆蓋範圍
Coverage Enhancements
 - 定位技術增強
Positioning Enhancements
 - 側鏈技術演進
SL Evolution
- 額外由RAN2領導的專門主題
Additional RAN2-led Candidate Topics
 - 網路控制中繼器
NCR
 - 加強側鏈中繼技術
SL Relay Enhancements
 - 無人飛行載具/城市空中交通
UAV/UAM
 - 多用戶識別模組
MU-SIM
 - 廣播/群播
Broadcast/multicast
 - 使用者裝置聚合、協作、備用
UE aggregation, collaboration, and
backup
- 額外由RAN3領導的專門主題
Additional RAN3-led Candidate Topics
 - 增強構造
Topological Enhancements
 - 接取與回傳技術/毫微微蜂巢式基地台
IAB/WAB/Femto
 - 如：公共安全、緊急服務
E.g. ... for public safety/emergency services
 - 服務品質 (QoE)
- 其他Others
 - 增強學習協定疊/高速封包/第二層用戶平面
Learn protocol stack/High speed
packetization/Layer 2 UP enhancements
 - 增強RAN架構/接取層安全
RAN architectural enhancements/AS Security
enhancements
 - 網路/外層程式碼
Network/Outer coding
 - 增強輕量化/高可靠度和低複雜度物聯網
RedCap Enh./High reliability and low
complexity IoT
 - 網路測試即服務/高準確網路測試
TaaS(Timing as a service)/High Accuracy
Timing Service
 - 增強小數據傳輸
SDT enhancements
 - 增強長期演進技術
LTE enhancements
 - 更新動態使用者能力
Dynamic UE capability update
 - 其他Others

圖 97、3GPP RAN 第 19 版本標準研討會列舉安全議題

資料來源：請參閱附錄-參考資料^{5.6}

依據蘋果公司(Apple)對第 2 工作組-架構工作組(SA2 Working Group - Architecture, SA2 WG)的工作規劃提案如圖 98，其中與 SA3 WG 有關連的議題包括接取流量導向、切換和拆分技術(Access Traffic Steering, Switching and Splitting, ATSSS)、增強服務品質框架(Enhancements to QoS Framework)、基於 MASQUE 增強流量管理(Multiplexed Application Substrate over QUIC Encryption for Enhanced Traffic Management)、進一步增強型擴展實境服務與元宇宙、3GPP 接取的上層流量導向、切換和拆分技術(Upper layer traffic steering,

5.6 3GPP RAN Chair's summary of Release-19 workshop

switching and splitting over dual 3GPP access)、啟用 AI 與 ML 的無線電系統架構(System Architecture enablers for AI/ML Radio)、整合衛星通訊的 5G 系統(Integration of satellite in 5GS)與 ISAC 等。

主題	簡要說明和主要目標
接取流量、切換和拆分技術	簡化並最佳化ATSSS的部署場景並研究其他ATSSS增強功能。 主要工作任務包括： 1. 研究如何擴展MPQUIC引導功能以能夠引導、切換和分割non-UDP流量（TCP、IP、乙太網路流量）。 2. 研究如何放寬對MPQUIC轉向功能的不可信non-3GPP 接入的IPSec通道封裝的強制使用，如有必要，研究 ATSSS的新架構選項。 3. 研究如何使用分支點（IPv6 多重歸屬）或UL分類器支援MA PDU會話。UE不需要知道MA PDU會話是否正在使用UL分類器。 4. 研究如何支援到LADN建立MA PDU Session。
增強服務品質框架	增強5G QoS框架。 主要工作任務包括： 1. 研究如何增強5GS QoS框架，包括資料包過濾集定義和資料封包流描述，以便能夠識別QUIC流並為同一PDU 會話中的不同QUIC流提供差異化的QoS。如果IETF可用，提議的解決方案應基於IETF協議或此類協議的擴展。 2. 研究如何增強反射QoS，基於增強的5GS QoS框架為QUIC流創建資料包過濾器。 3. 研究如何放寬反射QoS的每包處理需求，以便UE能為SDF維持更高的吞吐量。 4. 研究如何擴展反射QoS的UE能力訊號以指示處理不同傳輸協定的能力。
基於MASQUE增強流量管理	利用MASQUE技術增強5G流量管理能力。評估UPF中的ATSSS MASQUE代理是否應在Rel-19中推廣。 主要工作任務包括： 1. 研究5GC使用者平面中的MASQUE功能是否以及如何透過完全加密流量的明確資訊交換來使5GS流量管理受益。該研究確定了將公開的相關資訊。 2. 研究5GC使用者平面中的MASQUE功能是否以及如何使其其他5GC功能受益，例如報告使用者平面資料作為分析的輸入或監控UE中正確的URSP實作。 3. 研究如何向UE通告MASQUE能力，以及需要提供給UE哪些資訊。 4. 研究如何整合到PCC框架中，以及PCC框架需要哪些增強功能（如果有）。
進一步增強型擴展實境服務與元宇宙	進一步增強了Rel-18定義的PDU集合處理和UE節能功能。 符合SA1對行動Metaverse服務的新Rel-19要求。 主要工作任務包括： 1. 研究增強PDU集處理、N6上針對帶有加密RTP標頭的 RTP流的PDU集識別，支援除RTP/SRTP之外的更多協議，例如HTTP/DASH、QUIC。 2. 研究增強支援非3GPP接取、非3GPP接取中的L4S、PDU集相關的QoS控制機制擴展到非3GPP接取。 3. 研究XRM上行鏈路QoS和節能的改進。 4. 研究多路存取支援、XRM的MA-PDU會話、多路徑協定對端對端擁塞控制(L4S)的影響。 5. 支援行動Metaverse服務的增強型基於XR的服務。

主題	簡要說明和主要目標
3GPP接取的上層流量、切換和拆分技術	增強5G系統架構，解決MA PDU會話如何同時支援兩個3GPP存取路徑的問題。 主要工作任務包括： 1. 研究UE選擇初始PLMN後，在不同3GPP網路的情況下如何選擇第二PLMN或SNPN。 2. 研究如何加強註冊和會話管理程序。UE可以註冊到單一-PLMN、單一-SNPN、兩個不同的PLMN或SNPN、或一個PLMN和一個SNPN。 3. 研究如何支援單3GPP接入的PDU會話和雙3GPP接入的MA PDU會話之間以及雙3GPP接入的MA PDU會話之間的移動性。 4. 當UE透過多個NR接取和可能的一個非3GPP接取同時註冊到5GC 網路時，研究必要的增強功能以支援行動啟動和終止服務（例如，行動數據、語音、SMS、LCS）。 5. 研究如何擴展政策、引導功能和引導模式。
啟用AI與ML的無線電系統架構	研究如何增強5G系統以啟用AI/ML無線電。 主要工作任務包括： 1. 研究如何支援通用的5GS AI/ML框架以實現AI/ML無線電。 2. 研究如何增強現有的UE資料收集框架，以滿足AI/ML模型訓練（針對RAN）的要求。 3. 研究如何支援模型傳輸/下發到UE。 4. 研究如何支援資料收集和模型傳輸/交付給UE的安全和隱私方面。
整合衛星通訊的5G系統	3GPP對5GS進行了進一步增強，以支援基於TR 22.865中引入的新用例的衛星存取。 主要工作任務包括： 1. 再生酬載通用架構研究。研究具有「飛行」嵌入式3GPP 功能的核心網路對介面、協定（行動管理、呼叫）的影響。 2. 支援不連續饋線鏈路連接。研究4G和5G的儲存轉發通訊方案對介面和協定的具體影響。 3. 研究增強不連續衛星覆蓋、尋呼、再生模式切換最佳化的移動性管理。 4. 5GS的UE-衛星-UE通訊。研究UE-衛星-UE通訊的啟動、對會話管理、計費以及可能的監管服務的影響。
整合感知與通信	5G系統支援基於NR的感知功能，以使用NR RF獲取有關環境和/或環境內物體特徵的資訊（例如形狀、大小、方向、速度、位置、距離或物體之間的相對運動等）訊號。 重點工作任務包括： 1. 研究整體架構增強、支援感知服務所需的功能和程序。 2. 研究QoS模型和策略增強以支持多樣化的感知服務。 3. 研究感知服務授權以及感知結果向可信第三方的暴露機制。 4. 研究支援非3GPP感知資料和相關功能所需的架構增強和程序。

圖 98、Apple 提案 RAN 端安全議題

資料來源：請參閱附錄-參考資料^{5.7}

5.7 3GPP SA Release-19 workshop, SWS-230073

圖 99 是 Apple 對於 RAN 提出接取層安全性增強(Access Stratum (AS) Security Enhancement)，其需要強化的協定涵蓋呼叫(Paging)、系統資訊(System Information)、初次入網程序(Initial access procedure)、接取層安全機制啟動前的無線資源控制單播訊息(Radio Resource Control unicast message before AS security activation)、第 1 層網路訊息(L1 message)與第 2 層網路訊息(L2 message)。

- 目前的接取層安全性框架
 - AS 安全啟動後僅單播傳輸受到保護
 - 加密和完整性保護適用於每個PDCU SDU

Message types	NOTE	
呼叫(Paging)	PCCH	Unprotected
系統資訊(System Information)	BCCH	Unprotected
初次入網程序(Initial access procedure)	RACH procedure, CCCH message	Unprotected
接取層安全機制啟動前的無線資源控制單播訊息(RRC unicast message before AS security activation)	DCCH	Unprotected
接取層安全機制啟動後的單播訊息(Unicast messages after AS security activation)	DCCH, DTCH.	Protected
第一層網路訊息(L1 message)	PDCCH, PUCCH, PRACH, SRS, SSB/CSI-RS.	Unprotected
第二層網路訊息(L2 message)	L2 Control PDUs, L2 header...	Unprotected

- GSMA提出越來越多的安全風險案例

GSMALS	The risky case
R2-2106454 (Stealth Pirating Attack by RACH Rebroadcast Overwriting (SPARROW))	The risk during the RACH procedure
R2-2102607 (User location identification from Carrier Aggregation secondary cell activation messages (FSAG Doc 88_009; contact: GSMA))	The risk on SCell activation/deactivation MAC CE

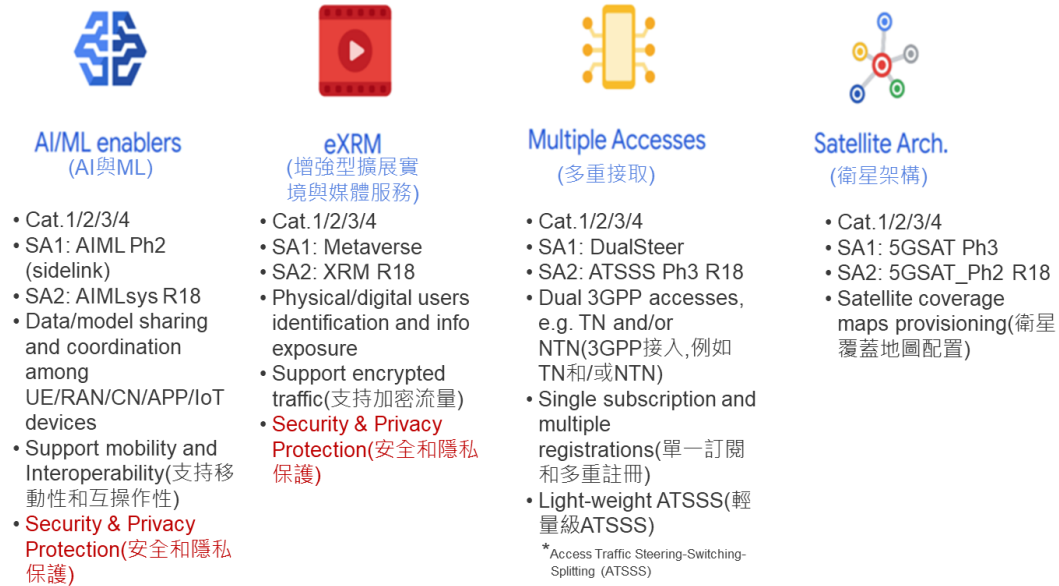
圖 99、Apple 提案接取層安全性增強

資料來源：請參閱附錄-參考資料^{5.8}

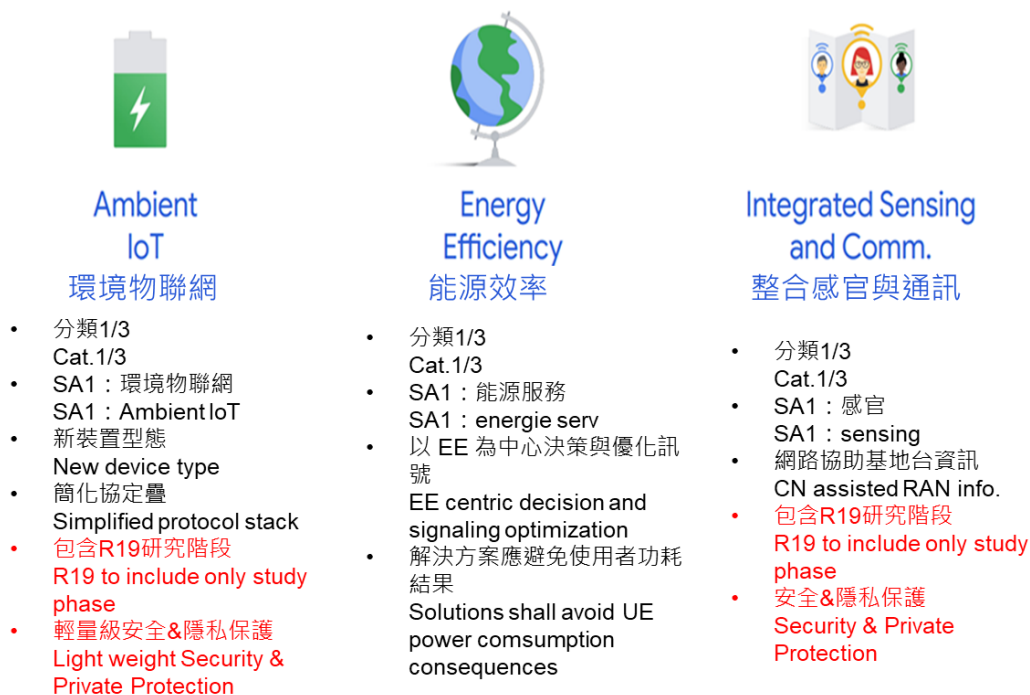
Google 在 3GPP 第 1 工作組-服務工作組(SA1 Working Group - Service, SA1 WG)與 SA2 WG 的工作規劃提案如圖 100，對於啟用 AI 與 ML(AI/ML enablers)、增強型擴展實境與媒體服務(enhancements for Extended Reality and Media services, eXRM)、環境物聯網(Ambient IoT)與 ISAC 等議題都需要重視安全及隱私保護。

5.8 3GPP SA Release-19 workshop, RWS-230463

● Google 優先級 R19 主題 (系統增強)



(a) 系統增強(Enhancement)



(b) 新服務(New Services)

圖 100、Google 新興服務重視通訊安全的工作規劃

資料來源：請參閱附錄-參考資料^{5.9}

MITRE 亦有對 SA2 WG 與 SA3 WG 工作規劃提案如圖 101，有關連的議題包括免除 SIM 卡驗證的專網系統(SIM-less Authentication for NPN)、端對端自我安全與強健網路切片(End-to-End Self Securing and Resilient Network Slices)、增強型 ATSSS、非地面網路增強(NTN Enhancements)等。

主題	簡要說明和主要目標
非公共網路 (NPN) 的無 SIM 身份驗證 SIM-less Authentication for Non-Public Networks (NPN)	5GS 應支援營運商控制的替代身份驗證方法 (即 AKA 的替代方法)，並具有不同類型的憑證，用於隔離部署場景 (例如工業自動化) 中物聯網設備的網路存取。它還應支援適當的框架 (例如 EAP)，允許使用非 3GPP 身分和憑證的替代 (例如 AKA) 身份驗證方法用於 NPN 中的 UE 網路存取身分驗證。
端對端的自我安全和彈性網路切片 End-to-End Self-Securing and Resilient Network Slices	5G系統對E2E網路切片 (RAN、傳輸網路和核心網域) 的支援缺乏對自主安全的自我安全和彈性能力的支援，如： a) 當操作環境改變時，動態更新E2E網路切片能力； b) 自動確保跨網路場景的服務持久性。 E2E切片功能對於 V2X、新一代 (NG) 公共安全、急救人員和關鍵基礎設施等用例至關重要。
R19版本(Rel.19) ATSSS 的增強功能 Enhancements to ATSSS in Rel. 19	5GS 利用存取流量引導、交換和拆分 (ATSSS) 來實現資料傳輸技術。最近，3GPP的 SA1和 SA2技術工作群組一直在致力於從不同角度進行可能的改進的創新解決方案，關鍵工作任務包括定義：(1) MPQUIC；(2) IPv6多路徑的使用；(3) UL (上層)、LL (下層) 轉向能力。
針對 Rel-19 及更進階版本的 NTN 增強功能 NTN Enhancements for Rel-19 and Beyond	研究 5G NTN 解決方案中新 E2E 服務的 5GS 要求衛星網路功能，例如衛星間連結、衛星到 HAPS 連接和衛星到地面通信，定義 E2E關鍵工作任務包括：(1) 指向、捕捉、追蹤相關的服務需求；(2) 這些服務的資料包將如何轉發；(3) PNT啟用的同步和時間戳要求服務；(4) 研究 OISL(衛星鏈路) 在提供 5G 與5G以上規格時，具有嚴格安全性、低延遲和高可靠性的服務吞吐量需求。

圖 101、MITRE 的工作規劃

資料來源：請參閱附錄-參考資料^{5.10}

總結而言，6G 時代預期將於 2030 年到來，6G 系統急切需要一套確保 IoT、異構雲端網路、設備、子網路和應用服務全面性推動安全技術。6G 威脅面向將由 6G 架構定義分解、開放接口具有多個利益相關者的環境，分解進入網路彈性、隱私、信任領域及其各自交叉點，3GPP 會員廠商們持續探索相關的安全技術推動因素，包括自動化系統創建自動化封閉環境安全操作、隱私保護技術、硬體、雲嵌入式信任架構和 DLT 網路層安全防護，AI/ML 作為關鍵技術推動因素，整個安全技術堆疊和相關性架構設計將變得普遍且至關重要。

5.9 3GPP SA Release-19 workshop, SWS-230069

5.10 3GPP SA Release-19 workshop, SWS-2230027

第二節 探討我國 6G 資安服務框架與推動機制

一、我國通訊產業 6G 發展現況

臺灣現有工業電腦與伺服器廠商以及小型基地臺製造商，積極投入 O-RAN 架構以及邊緣運算平臺網通設備的市場，而且營運商為節流、切割標單及分開採購，直接向品質佳的第三方設備供應商購買，網通設備「白牌化」商機應運而生。當企業欲建立起專網環境時，可透過租用電信營運商的網路達成，但礙於企業的資訊需要保密，故需要將邊緣運算平臺部署於企業網路中。為實現低延遲率與高可靠度以及高傳輸速率的垂直領域應用服務，需將 6G 專網多接取邊緣運算與電信業者 RAN 及核心網路的通訊設備緊密整合，所以 6G 專網多接取邊緣運算是未來部署 6G 企業專網的關鍵。

將隨著電信公司逐步擴大採購國產的 O-RAN 設備，O-RAN 架構帶來全新、額外的接觸點，以及軟體和硬體的脫鉤，導致技術天生就不安全。歐洲執行委員會在開放式無線接取網路研析報告(Report on the cybersecurity of Open RAN)亦點出 O-RAN 架構開放介面的安全議題，並將 O-RAN 的風險評估納入歐盟 5G 工具箱(EU 5G Toolbox)之中。

O-RAN 的集中單元(Central Unit, CU)涉及到 UE 之控制平面(Control Plane, CP)與使用者平面(User Plane, UP)封包的完整性和機密性。而分散單元(Distributed Unit, DU)與無線電單元(Radio Unit, RU)不會涉及到 UE 的完整性和機密性，但當其遭受攻擊時仍然會影響 UE 的可用性。

針對上述日益顯著資安議題，O-RAN Alliance 的安全工作小組(Security Working Group, SWG)針對 O-RAN 開放式架構的安全確保機制，將採用 GSMA 制定的 NESAS 搭配 3GPP 制定的 SCAS，NESAS 方案實施作法已詳述於第一節。

目前發展狀況來說，以兼有硬體和軟體開發專業能力的廠商，是最典型的 O-RAN 系統整合商，但幾經跨域合作和自行研發的努力下，軟體專精和硬體專精的廠商也藉由推出高度整合性解決方案，試圖在系統整合角色卡位；電信營運商為能更徹底的控制整合品質和成本，設法自行建立系統整合能力，也具備了轉型成為系統整合商的基礎，2023 年 O-RAN 全球 PlugFest 是 O-RAN Alliance 第 5 次的全球測試和整合活動，主要在於展示 O-RAN 生態系統的實力，本年度全球場域共計 10 處，超過 60 家廠商參與，其中我國由耀睿科技第三方公正實驗室(Open Testing and Integration Centre, OTIC)完成 24 家廠商(多數為國內廠商，如仁寶電腦、和碩聯合科技、雲達科技、亞旭電腦、神達、英業達、工研院、資策會...等)互通或安全性測試，占全球總數 40%，廠商參與除了顯示對開放架構的支持和投入外，也表示有越來越多廠商了解到開放架構下，符合電信商需求的設備應該如何設計，在國內通訊軟體和系統整合等能力發展成熟之前，白牌設備或者客製化代工仍是我國通訊硬體廠商應積極爭取的商機，而要打入國際電信商的供應鏈中，必須盡快設法與國際市場上主導開放架構布建的系統整合商建立硬軟優勢互補的合作關係。

本計畫綜整國際趨勢研析以及我國現況盤點，研提以下建議供參：

臺灣現有工業電腦與伺服器廠商以及小型基地臺製造商，應強化對 3GPP 及 O-RAN Alliance 標準規格及關鍵技術之掌握，可依據 O-RAN Alliance 的方案，以 GSMA 制定的 NESAS，搭配 3GPP 制定的 SCAS 來驗證產品安全性，於設計階段降低產品於商用時的資安修補成本，除了可以滿足潛在客戶資安需求外，同時亦可提升產品的國際市場競爭力。

二、提高 6G 網路安全性和隱私保護建議

6G 與 5G 的最主要差異在於全方位通訊與智慧化，5G 技術用於陸上通訊為主，6G 更進一步的擴展天空與海洋，讓世界不再有偏鄉

通訊不佳的問題，也讓遠洋漁船甚至海底的作業都能進行無線通訊與連網。國家科學及技術委員會已於 110 年起規劃「6G 前瞻布局」將擴大 6G 科技投入，連結我國晶片半導體與太空發展，於現有的 5G 及低軌衛星通訊基礎上，投入 6G 次世代通訊前瞻布局，同時重視資安防護機制，形成以智慧化高可靠度為主軸的新興產業生態系，維持臺灣在資通訊產業的領先地位。

綜觀我國政府針對資安產業的規劃，近年間越發積極且細緻，包括目標、主(協)辦機關及應對措施皆清楚列定，惟在技術發展應用的過程中，全球與我國皆面臨同一個現象，現今疊加如 OpenAI 推出 ChatGPT 聊天機器人的應用，各國政府亦意識到應制定規範 AI 科技的相關政策。亟需透過跨部會整合，包含大數據、個資保護、隱私、資安等相關法規加在一起，逐步解決配套措施未臻完備等問題。本計畫綜整國際趨勢研析以及我國現況盤點，研提以下建議供參：

(一)透過政策與產業研究，針對產業發展癥結著手。

(二)任何政策的擬制自不能脫離產業實際需求，亦不應憑空而生，

以美國白宮於今(2023)年 4 月召開會議，會後發布「6G 原則：透過設計實現開放和韌性(Principles for 6G：OPEN & RESILIENT BY DESIGN)」，內容強調美國需要打造一個具全球競爭力、安全和包容性的 6G 生態系統。該生態系統優先考慮可負擔性、可近用性、永續性和隱私保護，所發布的 6 點原則中「原則三、注重安全、彈性和隱私保護—打造具有網路安全系統的無線通訊系統，包括安全設計、基本服務的可用性、具有安全故障和快速恢復的系統，以及可靠、有彈性並保護用戶隱私的無線通訊系統。」已將網路安全與資料隱私列為關鍵要素之一。亦強調政府與學術界、業界和社會的利益相關者之間為實現目標而進行合作的重要性，持續透過政策制定、落實、成效評估與修正的循環，優化資安防護體系。爰此，本研究建

議我國亦可透過以下方式盤點我國現行面臨風險並進一步釐清產業需求，具體作法包括：

1. 訪談資安業者，了解相關業者面臨的障礙與機會，以做為扶植 6G 資安業者之依據。
2. 分析各國扶植 6G 資安業者的政策規範、市場概況與先天優勢，以做為扶植 6G 資安業者政策之依據。
3. 研析各國資安業者成功模式，供我國資安業者參考，裨益我國資安業者與國際市場接軌。
4. 定期執行資安市場調查，以檢視政策具體成效，循環調整相關政策。
5. 創造資安防護需求，整備制度環境本計畫訪談中，許多業者反映我國資安產業面臨最大發展瓶頸係「防護意識不足」、「缺乏防護誘因」等，簡言之便是需求面的不穩定使供應面發展同步受限，爰此創設需求成為我國資安產業發展的關鍵要素。

此外，縱有法規规范要求特定業者，如提供 5G 服務電信業者落實資安防護規劃，惟倘法規规范架構不明確或法規规范過於細節皆可能阻礙產業發展，前者恐造成法遵成本提高且各業者對資安防護認知歧異；後者恐限制產業創新應用等，因此相關政策的擬制除應審慎為之，更應動態調整，以因應產業實務。

三、我國 6G 資安推動機制

6G 做為延續 5G 技術下世代通訊技術，預期將彙集資通訊、資工、半導體、材料科學等領域建構新世代 6G 網路，相較於 5G 網路，所需科學領域更為廣泛，其中虛實整合趨勢更具備衍生各項創新應用的潛力，就目前現況而言，業者從 5G 發展有明確需求及發展潛力之應用市場，將成為業者 6G 重點發展方向。

本計畫針對目前正在發展的 5G 專網需求及邁向 6G 挑戰，與台灣電信產業發展協會、電信系統整合商及網通業者進行技術的交流討論，多數業者毫不諱言，由於 5G 高頻寬、低延遲及大連結的特性，確實為通訊帶來商機，連帶地也領航 5G 產業供應市場對資安的需求，尤其 MEC、第三方間接業務及 5G 企業專網為未來 5G 商機延伸項目的資安風險與挑戰；具體而言，5G 商用後於企業專網市場相當大，且由於市場剛開發，客戶、設備商及服務商等，皆有共識採用開放性的架構無縫接軌至 6G 系統服務，業者會有更大的意願與資安廠商合作，資安廠商能有較大發揮空間，以多元貨量身訂製的方式滿足客戶需求，尤其以 O-RAN 基站設備商、邊緣運算及伺服器等業者，皆為資安廠商可以合作的對象，並認為我國在技術整合和對接測試具有先天優勢。

綜整本研究研析成果，提出以下建議供參：

- (一)研擬 5G 延伸到 6G 建立相關資安標準規範，以多邊組織與國際先進國家發布之標準為依據，以確保我國通訊環境之韌性與安全性，裨益我國業者進入國際 6G 供應鏈。
- (二)建立企業 6G 資安防護框架，並追蹤企業落實狀況，以確保我國企業有統一框架可循，如制定 6G 供應鏈資安指引，納入技術性與非技術標準，確保我國通訊產業供應鏈乃至 6G 環境之安全性。
- (三)提供誘因，創設我國企業資安需求，如由學研機構建立更多 6G 實驗共創場域，以協助我國業者執行資安檢測與驗證。
- (四)建議我國於 6G 技術設計研發階段，發展群聚科技生態系的特性，研析最可能且實質發展之面向，例如人口老化趨勢不易短時間逆轉，相應衍生需求議題發生可能性較高，發展群聚科技生態系的特性，透過長期且持續性觀測，累積充足研析資料，推進未來 6G 發展方向。



資安產業做為我國 6 大核心戰略產業之一，近年產官學界投入越來越多的資源在該領域，惟資安產業的投資應有明確目的、方向且具體可行，否則恐使相關投資膨脹、泡沫化，爰此，持續觀測國際趨勢，並尋求我國發展契機乃我國當前關鍵課題。

第三節 6G 資安產業研析與防護實證應用驗測實證先導評估

一、實證目的

6G 應用領域的演進需要超越當前網路設計的創新網路架構，主要是開放分佈式參考框架包含動態雲服務的初始化與擴展、5G 核心網路基於服務架構延伸到 RAN，被稱為核心-RAN 融合，並可以協調核心功能與 RAN 建立更簡單的子網路且獨立運行，6G 將網路軟體化、雲服務化帶入網路智慧化，使無線網路從 IoT 到智慧物聯網 (Artificial Intelligence of Things, AIoT)，發生革命性的變化。這促使 6G 網路的端到端自動化需要主動發現威脅、AI 生成融合緩解資安技術，實現自我維運的網路系統。

由 2G、3G 發展出來的 GSM 系統之單向認證機制仍存在缺陷，從而讓假基地臺有機可趁，惡意人士透過假基地臺監測無線通訊系統中的各種訊令傳輸來竊取私密資料，進行盜用或詐騙，為此，GSMA 於 2019 年已經將惡意中繼站對行動通訊系統的中間人威脅 GSMA Doc CVD-2019-0024，列於協調性弱點揭露機制 (Coordinated Vulnerability Disclosure, CVD) 資料庫中，並督促 3GPP 安全性工作群組 (SA3 Security) 的國際標準會議中，針對假基地臺的安全威脅，請求在標準層面進行改善，定義一種威脅偵測機制來偵測假基地臺的存在，藉此保護行動通訊系統合法終端用戶的隱私安全性，Apple 在 3GPP 組織裏，正在主導進行「對抗第五代行動通訊技術假基地臺之安全增強型研究項目 (Study on 5G Security Enhancement against False Base Stations)」，預期在通訊標準更版裏，未來 6G 網路將可以排除假基地臺的安全威脅。

在檢視 6G 的安全威脅情況，由於 6G 系統的大規模分佈式特性，安全性較低的子網路有可能為攻擊者提供入侵系統的機會，進而使用滲透信任感染整個廣域網路，因應 6G 或 Pre-6G 網路架構發展趨勢，從 3GPP 國際標準規格，評估從 5G 繼承的安全問題，聚焦基地臺連

線核網之入網的身分驗證方式，介紹遺留在行動網路中的安全問題，提出 6G 應用安全問題並提出解決方案。

本計畫建立 5G 資安實驗室之軟硬體設備，按現行主要的國際標準 3GPP 探討技術規格方向，使用 Amarisoft 環境，並自行開發第六代行動通訊先期技術核心網路(Pre-6GC)、基地臺(gNB)與終端(UE)模擬環境，探討 3GPP 標準規格中遺留的身分驗證安全議題與緩解方案，本實證計畫能夠促使以下身分驗證方法持續探究：

- (一)網路訪問安全：6G 將使用基於雲服務和開放可調修網路技術，需要建立新的身分驗證方法。
- (二)網域連結安全：6G 將擴展到 NTN 等異質網路接取，需要建立開放身分驗證又可稽核驗證方法。
- (三)用戶端安全：運用身分驗證控制訪問機制是 6G 安全期待已久的功能，改善用戶體驗。
- (四)應用端安全：雙方必須對自己進行身分驗證，6G 信任網路才能運行。

技術實證結果對應 6G 關鍵性技術指標可靠性(Reliability)與安全和隱私(Security and privacy)，雖然目前有關 6G 無線通訊標準的資訊還很少，本團隊仍針對現行正在探討演進中的 6G 無線網路基礎架構元件的特性，實作避免使用者認證資訊產生洩漏風險，導致阻斷使用者應用無線網路服務，並防止假冒網路基地臺或攻擊者誘騙網路用者，產生隱私資訊洩漏，提升系統可信賴性與資料隱私安全。

二、測試方法

6G 設想實現 IoE，這可以想像為數十億異構設備的集合，目前依賴 SIM 卡基本設備安全模型，並不能滿足 6G 中的 IoE 實際部署，尤其是在如此龐大的網路中，密鑰分發和管理功能效率極低，而韌體資源有限的小型 IoT 設備無法承受複雜的加密技術，來維持強大的安全性，這成為攻擊者的主要目標，這些設備有可能受到損害並可能被利

用來發起攻擊，優先阻絕此類的設備對大範圍通訊網域的潛在安全威脅。

本計畫從論述以目前 5G 標準的通訊規格下，模擬 6G 或 Pre-6G gNB 與核網連線時，用戶端身分辨試與驗證的工作原理，提出「假核網+基地臺誘騙用戶攻擊」、以及「假用戶對核網的攻擊」等 2 大類型 4 種資安攻擊情境，分述假基地臺及假用戶連線的情境與危害，提出相應的緩解措施與安全標準的對策建議，如圖 102 所示。

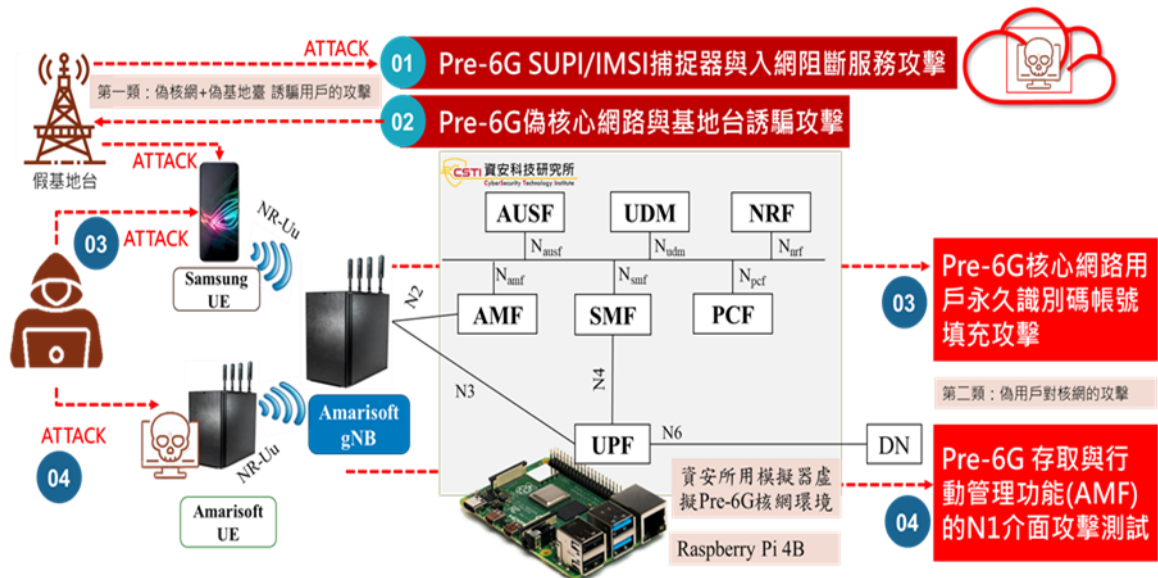


圖 102、模擬 6G/Pre-6G 基地臺與核網連線 2 大類型 4 種資安攻擊情境

資料來源：本計畫整理

6G 網路利用原生安全能力，結合 6G 強大的基礎設施來應對這種挑戰，是本次防護實證應用驗測實證先導評估主要研究的標的項目：

(一)假核網+基地臺誘騙用戶攻擊

傳統的網路攻擊行為往往伴隨著 IP 欺騙，當面對這種攻擊時，現有防禦系統將虛假的惡意地址放入黑名單，並不能做到有效的防禦。儘管有研究提出 IP 回溯技術來解決攻擊中的 IP 欺騙，但在實

際應用中存在許多問題，尤其是在 6G 高速網路中，面對 DDoS 伴隨 IP 欺騙攻擊時，需要消耗路由器的大量儲存和運算資源。

(二)假用戶對核網的攻擊

6G 網路的峰值速度將達到 Tbps，在長期監控流量時，為掌握每個流量的狀態，將對儲存和運算資源帶來嚴峻挑戰。因此，現有的檢測方法可能不適用於 6G 高速網路中檢測慢速 DDoS 攻擊這類攻擊行為，且 DDoS 攻擊不再局限於單一類型的攻擊，通過幾種類型結合，來發起混合攻擊，增強攻擊的欺騙性及隱蔽性。

三、6G 資安技術與 ISO 27001 控制項目對應

因應新型態的駭客攻擊樣態，ISO 已於 2022 年 2 月 15 日公布最新版本 ISO/IEC 27001：2022「資訊安全、網路安全與隱私保護」與 ISO/IEC 27002：2022「資訊安全控制措施」，內容包含 4 個控制主題，14 個控制領域，共計 93 項控制措施，2022 版的控制措施能看出資訊安全管理的範疇，亦著墨於網路安全與隱私保護的管理。

數位轉型、5G 時代，數位化的資料數量越來越多、網速越來越快，組織因應新版 ISO 27001 的 4 個控制主題要求時，基礎資安更應該對照 ISO 27001 資安措施，避免影響資訊傳遞的機密性 (Confidentiality)、完整性(Integrity)與持續運作，「6G 資安產業研析與防護實證應用驗測實證先導評估」設計 2 類 4 種資安測試實證，其緩解措施與 ISO 27001 控制措施關聯如表 38，對應 ISO 27001 之控制措施與合規建議，促使 Pre-6G 系統於規劃期間，能夠應對日益複雜的安全風險，確保營運持續並獲得競爭優勢。

表 38、4 種攻擊類型之緩解措施與 ISO 27001：對應控制項目組

類型	網路威脅說明	緩解措施	ISO 27002:2022對應控制
第1種：Pre-6G SUPI/IMSI捕捉器與入網阻斷服務攻擊	假基地臺(Pre-6G gNB)實現中間人攻擊 Pre-6G核心網路透過回復拒絕註冊(Registration Reject)訊令，達成用戶對阻斷服務(Denial of Service, DoS)攻擊	在電信系統加Operator身份合法確認機制	A.5.30 營運持續之ICT備妥性 A.8.16 監視活動
第2種：Pre-6G假核心網路與基地臺誘騙攻擊	發送Null Security方式規避加密與完整性檢查，達成後續的入網程序	檢測用戶設備(UE)安全設定設為不支援5G-IA0	A.5.30 營運持續之ICT備妥性 A.8.9 組態管理
第3種：Pre-6G核心網路用戶永久識別碼(Subscriber Permanent Identifier SUPI)帳號填充攻擊	Pre-6G核心網路用戶SUPI帳號填充測試方法	一律要求用戶設備進行入網身份認證	A.8.9 組態管理 A.8.16 監視活動
第4種：Pre-6G存取與行動管理功能(AMF)的N1介面攻擊測試	AMF模組中存取安全標準規格是否齊備，若有未完成，可能直接造成設備已知弱點，容易成為零日攻擊(zero day)的破口	落實6G核心網路通訊安全測試評估	A.5.30 營運持續之ICT備妥性

資料來源：本計畫整理

綜整上述 6G 資安技術對應 ISO 27001 之控制措施與合規建議之外，隨著 6G 系統之 AI 技術及其應用不斷擴增與發展，為使可信賴的 AI 技術得以標準化，亦須觀注 2018 年 ISO 和國際電工委員會(International Electrotechnical Commission, IEC)在其資訊技術聯合技術委員會(ISO/IEC JTC 1)下，成立人工智慧小組委員會(SC 42)，主要負責 AI 領域方面的標準化，而美國的 AI 法制化也在進行中，如 2020 年 NIST 發布 Artificial Intelligence Risk Management Framework 標準來支持 AI 所需要的風險管理作業，加拿大與歐盟正在制定 AI 法令(AI Act)聚焦高風險或高衝擊 AI 系統的風險對應策略與確保 AI 持續監控，相關國際標準的發展，促使可信賴的人工智慧目標得以實現，以下簡單介紹 AI 技術與管理之國際標準發展進程：

ISO/IEC 38507:2022(Governance implications of the use of artificial intelligence by organizations；組織運用 AI 技術資訊治理影響)於 2022 年 4 月已公告第一版，文件的範圍涉及 AI 的使用對組織的影響，AI 的使用帶來新的風險和責任，應由使用它的組織予以解決。

ISO/IEC FDIS 42001：2023 (Artificial intelligence Management system；AI 管理系統)正在發展中，目前在國際標準最終草案版，是針對 AI 的管理系統標準，提供可認證的 AI 管理系統框架，文件目標在協助組織執行 AI 系統管理的角色，指導組織如何管理(包括建立、部署、維護、持續改善)，提高 AI 應用的品質、安全性、可追溯性、透明度和可靠性，並向利害關係人保證系統正在負責任地開發。

ISO/IEC CD 42005 (AI system impact assessment；AI 系統衝擊評鑑)正在發展中，目前為委員會草案版，是針對組織對可能受 AI 系統及其預期或可預見應用影響的個人和社會，進行 AI 系統影響評估，內容包括在 AI 系統開發生命週期的哪些階段，如何及何時執行此類評估與注意事項，完成 AI 系統影響評估文件的指南，同時還包括如何將此 AI 系統影響評估流程，整合到組織的 AI 風險管理和 AI 管理系統中。

ISO/IEC 38507 是組織對 AI 技術的管理政策與原則，ISO/IEC 42001 是系統開發流程相關風險管理量測控制措施，ISO/IEC 42005 則是識別組織內涉及 AI 相關系統、或是高風險高衝擊的 AI 系統範圍，進行 AI 風險評鑑，對於不符合與潛在不符合項目持續改善，透過 ISO/IEC DIS 42006 提供 AI 管理系統驗證與稽核機構的要求事項(即認證規範)，合成一套國際社會可遵循的完整驗證與認證機制，具體運用於 6G 系統應涵蓋的 AI 管理控制措施，尚待 ISO/IEC 42001、42005 正式版公告，再與高度相關的 ISO 27001(資訊安全管理系統)充分整合成整合式的資訊管理系統，提供資訊系統良好的安全管理監督機制。

四、測試環境及架構

本實證計畫利用資策會資安所所屬「通訊資安實驗室」環境執行，「通訊資安實驗室」提供開放並可互操作 5G 安全網路架構，經過資安相關的測試，建議供應鏈上應採取符合國際規範之安全管理策略及軟體更新流程與部署注意事項，以降低資安風險與威脅，讓產品或服務具韌性且安全。

依據 3GPP Release- 17(R17)完成 5G 通訊基本架構，在此基礎上參考 3GPP 最新研議 R18，開發模擬器中網路元件與介面，試做強化動態頻譜分享功能，允許上下行非對稱無線載波聚合，(R)AN 模組新增功能在頻段壅塞時候，透過 AI 技術支援彈性切換載波，3GPP R18 通訊系統架構如圖 103 所示，因其將行動無線通訊技術由傳統通訊架構轉向應用架構，業界普遍認為是向 Pre-6G 演進的重要一步。

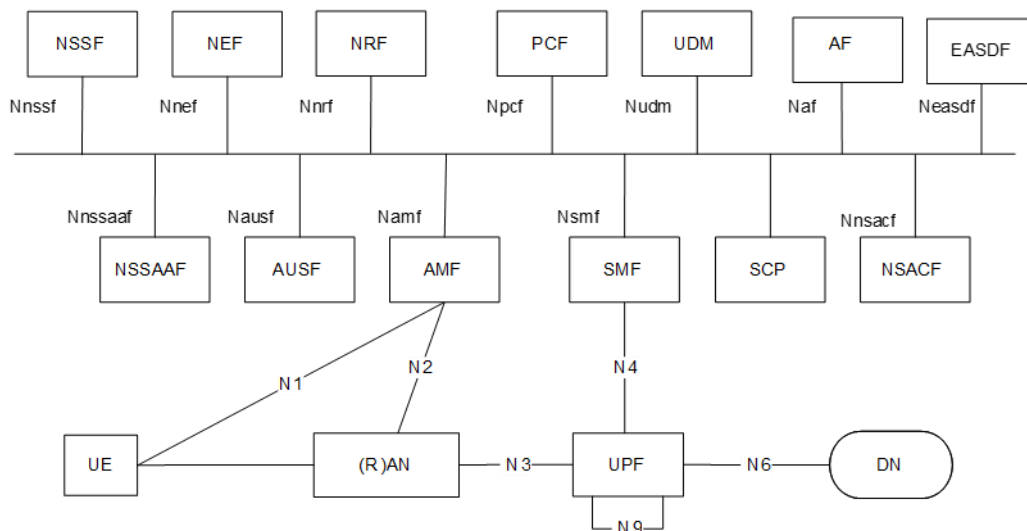


圖 103、Pre-6G 網路元件模擬器與實驗架構圖

資料來源：3GPP TS 23.501 V18.3.0

本計畫開發 Pre-6G 網路元件模擬器其中 Pre-6GC 包含 UPF、AUSF、SMF、存取與行動管理功能(Access and Mobility Management

Function, AMF)、統一資料管理功能(Unified Data Management, UDM)與網路資料庫功能(Network Repository Function, NRF)。而 gNB 與 UE 模擬器，包含 Pre-6G gNB N2 介面、N3 介面功能及 Pre-6G 終端(UE)的 N1 介面功能模擬，Pre-6G 網路元件模擬器與實驗架構如圖 104 所示。

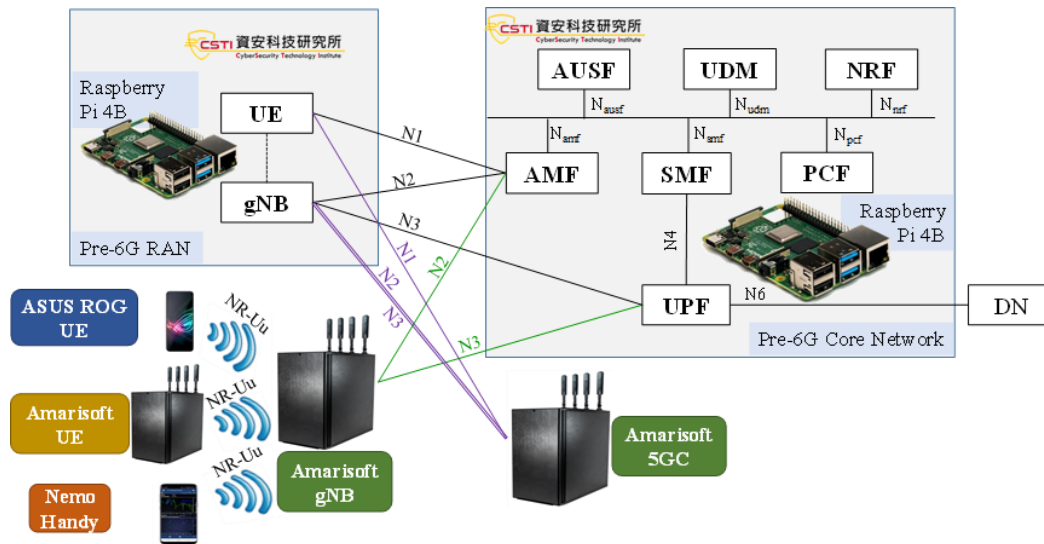


圖 104、Pre-6G 網路元件模擬器與實驗架構圖

資料來源：本計畫整理

測試系統環境設定，如硬體、作業系統選擇等具備以下要件：

- (一)通訊模擬設備選擇：採用 Amarisoft 軟體核心網路、Amarisoft 軟體 gNB 與 Amarisoft 軟體 UE，如圖 105 所示。



圖 105、Amarisoft 軟體核心網路及 gNB (左)與軟體 UE (右)

資料來源：本計畫整理

(二)作業系統和開發環境：採用 Raspberry Pi 4 Model B / 8GB 樹莓派第 4 代單板電腦，透過 Python 3 程式語言撰寫，自行開發的 Pre-6GC、gNB 與 UE 模擬器。

(三)資料收集和函式庫：自行開發的 Pre-6GC、gNB 與 UE 模擬器之通訊底層函式庫採法國資安廠商 P1 Security 提供 Python 3 函式庫模組(如 ASN.1 等)，模擬器操作介面如圖 106(Pre-6GC)與圖 107 所示(gNB 與 UE)。

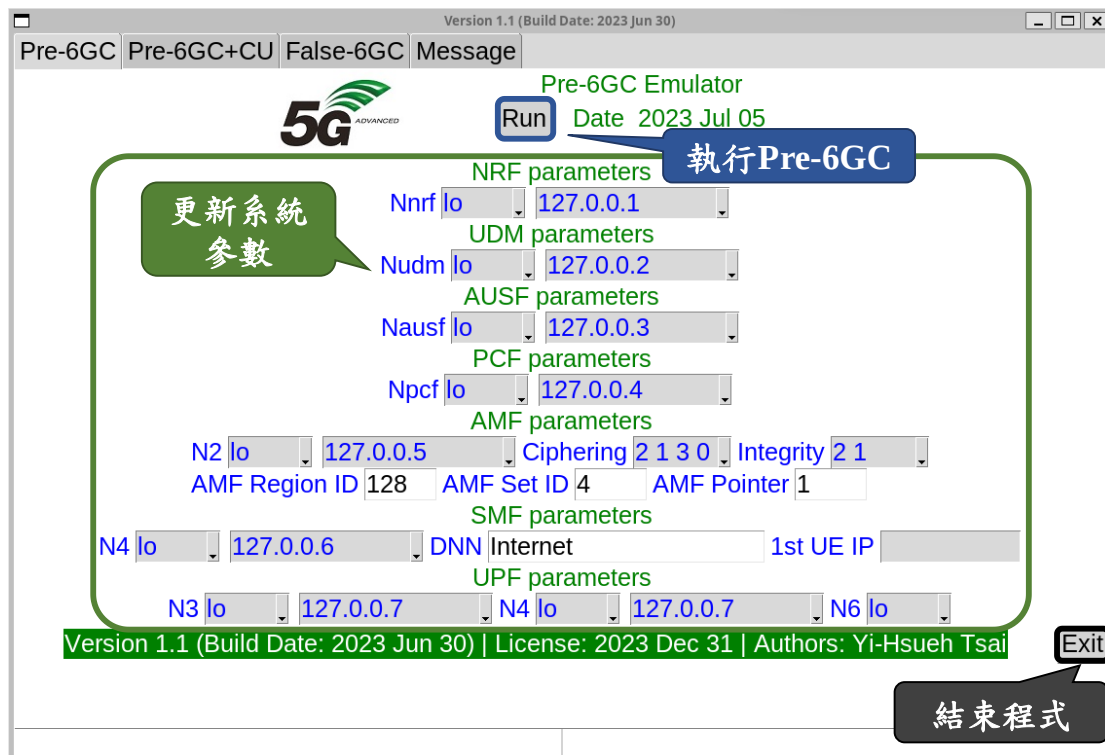


圖 106、Pre-6GC 模擬器操作介面圖

資料來源：本計畫整理

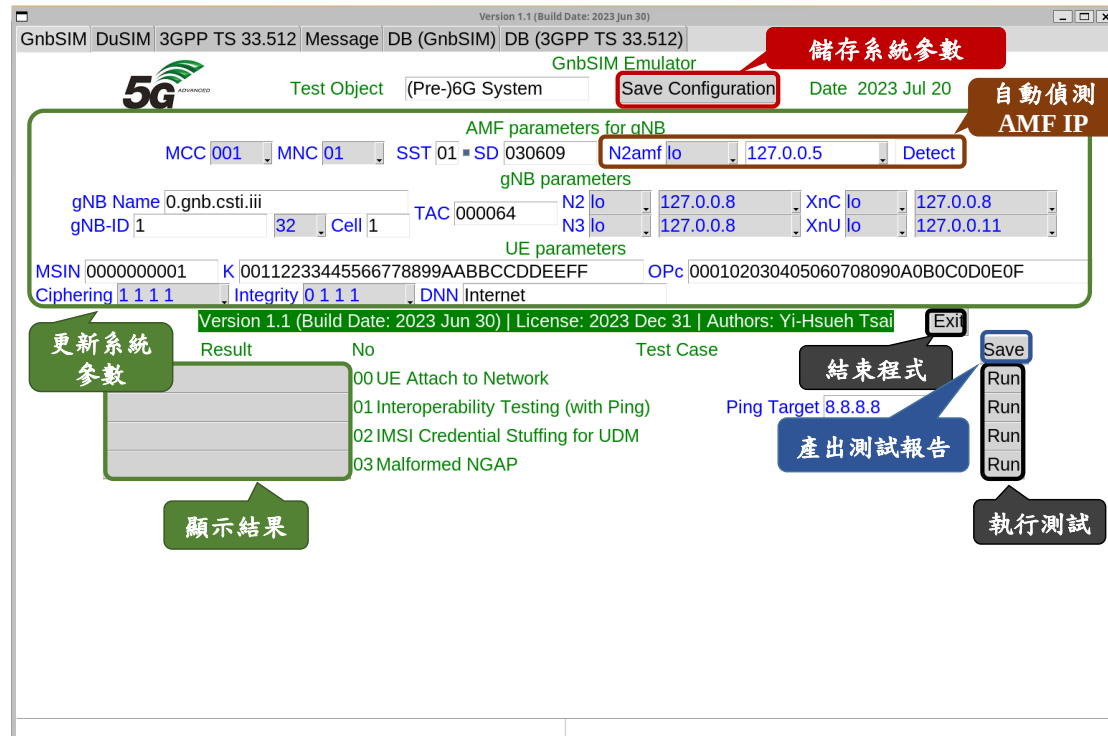


圖 107、Pre-6G gNB 與 UE 模擬器操作介面圖

資料來源：本計畫整理

(四)模型工具部署：模擬 Pre-6GC 與 gNB N1 介面、N2 介面、N3 介面可能分別遭受攻擊，搭建對應 Pre-6G 介面勾勒資安樣貌，確保測試過程中監控並截取測試數據。

五、使用之軟硬體規格

本次實驗以 Amarisoft 的通訊網路模擬器方案為基礎，提供包括核網、基地臺端到端軟體模擬環境，支援 3GPP 標準規範，搭建一個完整的 LTE/Pre-6G 網路。AmariSoft 軟體核心網路及 AmariSoft 軟體 gNB 規格如圖 108 所示，AmariSoft 軟體 UE 如圖 109 所示。

<i>eNodeB/ng-eNodeB Technical Specifications</i>	
3GPP release	LTE release 16
Frequency bands	All FDD and TDD bands in sub-6GHz
Bandwidth	1.4, 3, 5, 10, 15 and 20 MHz in LTE 200 KHz for NB-IoT supporting all operation modes (in-band, guard band and standalone).
Number of active UEs	Up to 1000 UEs distributed within the configured cells
Transmission modes	1 (single antenna) to 10 (MIMO 4x4)
Carrier aggregation	Up to 8 carriers in DL and 3 in UL allowing mixed FDD/TDD combinations in DL
Modulation schemes	Up to 1024QAM in DL and 256QAM in UL
AS encryption and integrity protection	AES, SNOW3G, ZUC
Handover	Intra eNodeB, S1, X2, Intra ng-eNodeB, NG, Xn and EPS to 5GS handover support
eNodeB network interfaces	S1AP and GTP-U to EPC X2AP between eNodeBs M1 and M2 for eMBMS
ng-eNodeB network interfaces	NGAP and GTP-U to 5GC XnAP between ng-eNodeBs
IoT	LTE category 0 and 1 LTE-M cat M1 FDD, HD-FDD and TDD support NB-IoT single-tone and multi-tone cat NB1 and NB2 NTN Rel17 NB-IoT
NB-IoT subcarrier spacing	15 kHz and 3.75 kHz

圖 108、Amarisoft 軟體核心網路及 gNB 規格

資料來源：Amarisoft^{5.11}

5.11 AMARI UE Simbox E Series. Retrieved from
<https://www.amarisoft.com/app/uploads/2022/03/AMARI-UE-Simbox-E-Series.pdf> (Mar. 03, 2022)



UE Simulator 4G technical specifications

3GPP Specification	LTE Release 8 support with features up to Release 15
Frequency bands	All FDD and TDD sub-6GHz bands from 500 MHz to 6 GHz with support of custom frequencies
Bandwidth	1.4, 3, 5, 10, 15 and 20 MHz, 200 KHz for NB-IoT
Carrier aggregation	up to 4 carriers in DL and 2 carriers in UL
MIMO	DL MIMO support up to 4x4
Modulation schemes	up to 256Q AM in DL and UL
AS encryption and integrity protection	AES, SNOW3G, ZUC
Handover	Intra-freq, inter-freq and inter-band Handovers
Group communication	eMBMS as per Rel10
IoT	LTE category 0 and 1, LTE-M cat M1, NB-IoT cat NB1 and NB2 UE categories
UE categories	Cat0, Cat1, cat 3, cat 4, cat 15 with 4CCs in DL and cat 13 with 2 CCs in UL
Number of active users	1000+ UEs (see table page 4 for details)
Number of active cells	4 cells MIMO 2x2 or 2 cell MIMO 4x4
IP traffic	Simulation of TCP, UDP, RTP, HTTP and VoIP with configurable packet size as well as support of external applications such as iperf

圖 109、Amarisoft 軟體 UE 規格

資料來源：Amarisoft^{5.11}

本次實驗自行開發 6G 網路模擬器的軟硬體規格如表 39 所示。

表 39、6G 網路模擬器軟硬體規格

名稱	6G 網路模擬器
硬體規格	• Raspberry Pi 4 Model B • ARM 架構處理器處理器 • 512MB RAM • 4 GB UFS
作業系統	Linux 系統
程式軟體	資策會_6G 核心網路(Pre-6GC)及 gNB 模擬介面
網路介面	RJ45 有線網卡
備註	(無)

資料來源：本計畫整理

5.11 AMARI UE Simbox E Series. Retrieved from <https://www.amarisoft.com/app/uploads/2022/03/AMARI-UE-Simbox-E-Series.pdf> (Mar. 03, 2022)

六、測試步驟

模擬 6G 或 Pre-6G gNB 與核網連線時，用戶端身分辨試與驗證的工作原理，提出「假核網+基地臺誘騙用戶攻擊」、以及「假用戶對核網的攻擊」等 2 大類型 4 種資安攻擊情境，由於是針對身分驗證程序的安全問題探究，4 種資安攻擊情境可能造成不同程度身分權限的安全威脅，亦有可能組合成為一連串的帳號設定疏漏，導致駭客可以多種利用，進而取得合法身分權限，可以控制或崩潰整個通訊網路。

(一)假核網+基地臺誘騙用戶攻擊

模擬 6G 跨領域應用環境，假基地臺可以透過「身分標識」的程序要求使用者提交國際行動用戶識別碼(International Mobile Subscriber Identity, IMSI)，一旦用戶回覆的明文 IMSI 資訊被駭客截取，就可用來追蹤和監視手機用戶，引發隱私外洩問題；進一步將截取到的 IMSI 資料尋找到的正式核網，若搭配在安全模式設定(Security Mode Command, SMC)中發送 Null Security 方式規避加密與完整性檢查，則達成後續的入網程序，蒐集核網串接資料流或展開內網攻擊情境。

1. Pre-6G SUPI/IMSI 捕捉器與入網阻斷服務攻擊

入網阻斷攻擊利用形式通常會導致行為緩慢、系統崩潰或其他有害的伺服器行為，從而造成阻斷服務。測試步驟如下：

- (1)本計畫實作假 Pre-6G 核心網路搭配假基地臺對終端用戶進行用戶永久識別碼(Subscription Permanent Identifier, SUPI)誘騙攻擊，透過該攻擊測試取得終端用戶的合法 SUPI，如圖 110 所示。

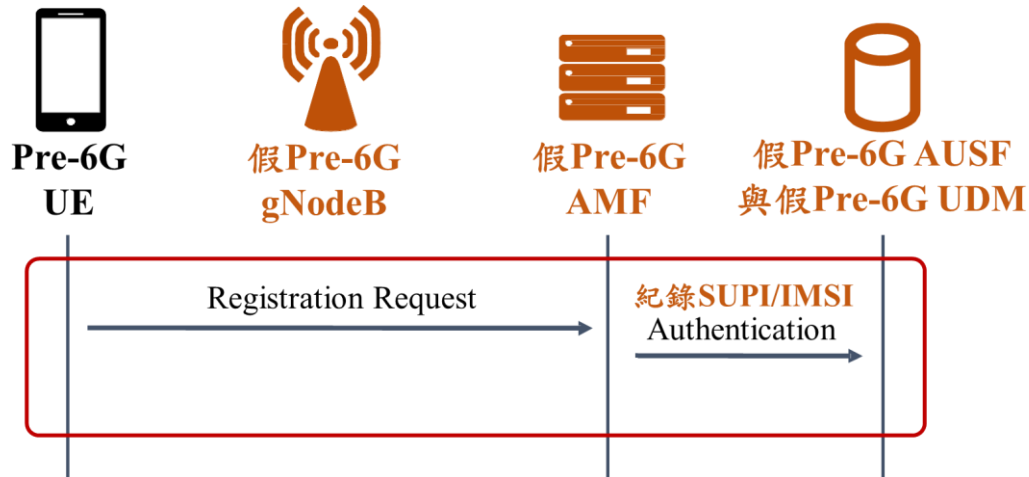


圖 110、Pre-6G SUPI/IMSI 捕捉器

資料來源：本計畫整理

(2)由於標準文件規定當用戶收到拒絕註冊(Registration Reject)訊令夾帶原因(Cause)為 Illegal UE 後，用戶必須進入 5G 待機模式(5GMM-DEREGISTERED)，如圖 111 所示。

(3)於完成終端用戶 Pre-6G SUPI/IMSI 捕捉後，Pre-6G 核心網路模擬器透過回復夾帶 Cause (Illegal UE)的拒絕註冊(Registration Reject)訊令，終端用戶無法上網的 DoS 攻擊。

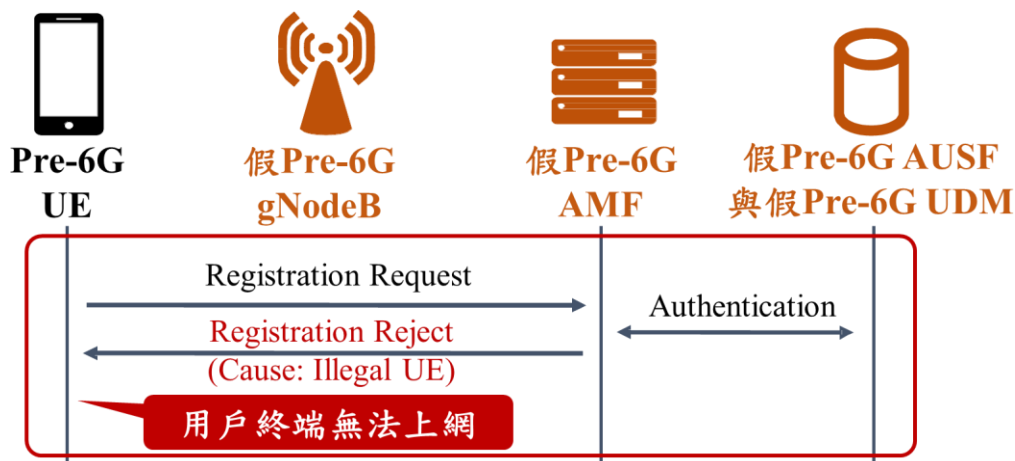


圖 111、透過 Illegal UE 實現入網阻斷服務攻擊

資料來源：本計畫整理

(4)由於標準文件規定當用戶收到夾帶 Cause (Illegal ME) 的拒絕註冊(Registration Reject)訊令後，用戶應當進入 5G 待機模式(5GMM-DEREGISTERED)。

(5)Pre-6G 核心網路模擬器透過回復夾帶原因(Cause)為 Illegal ME 的拒絕註冊(Registration Reject)訊令，通知達成終端用戶進入待機模式，如圖 112。

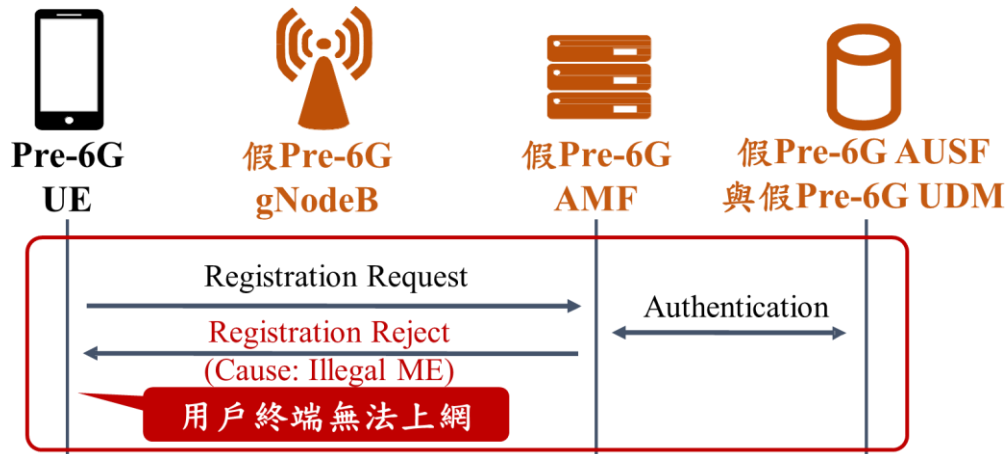


圖 112、透過 Illegal ME 實現入網阻斷服務攻擊

資料來源：本計畫整理

2. Pre-6G 假核心網路與 gNB 誘騙攻擊

誘騙攻擊是藉由騙取用戶端登入自身的帳號認證服務，對陌生應用程式進行授權，取得完整的身分驗證資訊，即可竊用受害者身分，進行內網橫向擴散攻擊，感染整個網路系統。測試步驟如下：

(1)本計畫實作誘騙終端用戶的實驗，由於 Pre-6G 入網認證用的認證向量(Authentication Vector, AV)並未加密，故可以透過網路分析器(Sniffer)獲得認證向量。並透過假 Pre-6G 核心網路搭配 gNB 發送重播認證向量，誘騙 Amarisoft 軟體用戶設備聯網通過認證程序，如圖 113 所示。接著搭配在 SMC 中發送 Null Security 方式規避加密與完整性檢查，達成後續的入網程序。

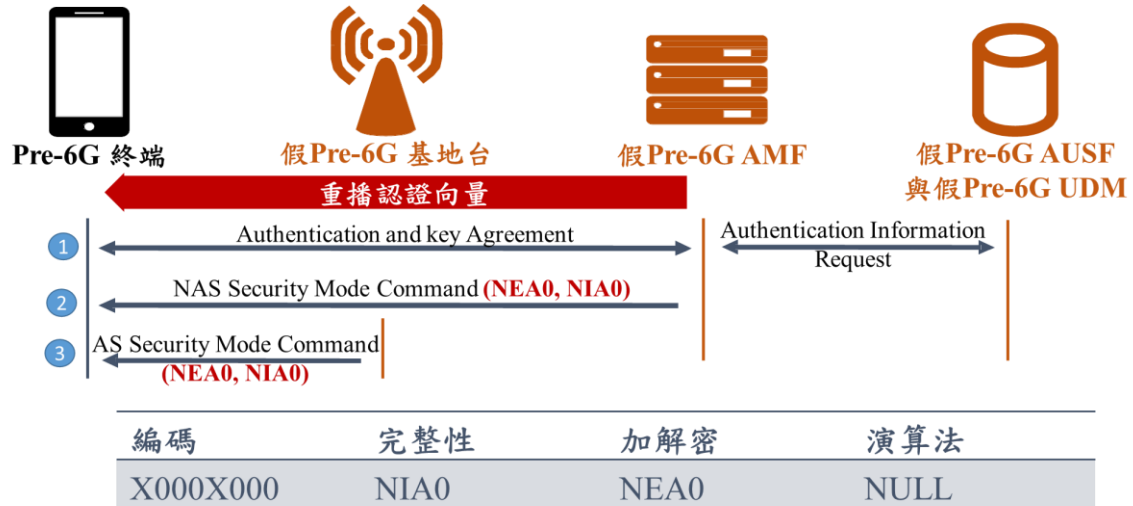


圖 113、Pre-6G 假核心網路與 gNB 重播 AV 的安全威脅

資料來源：本計畫整理

(2)接著實作跳脫終端用戶認證程序的實驗，透過假冒 Pre-6G 核心網路搭配 gNB 於接收到註冊請求 (Registration Request) 訊令後，跳脫認證程序直接發送 SMC 訊令中發送 Null Security，誘騙 Amarisoft 的軟體用戶設備聯網通過認證程序，如圖 114 所示。

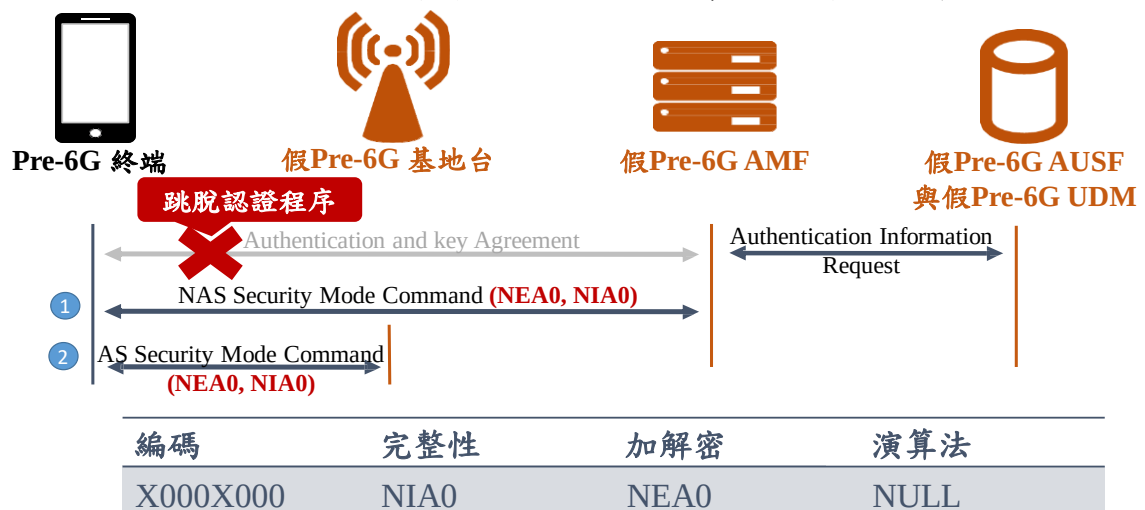
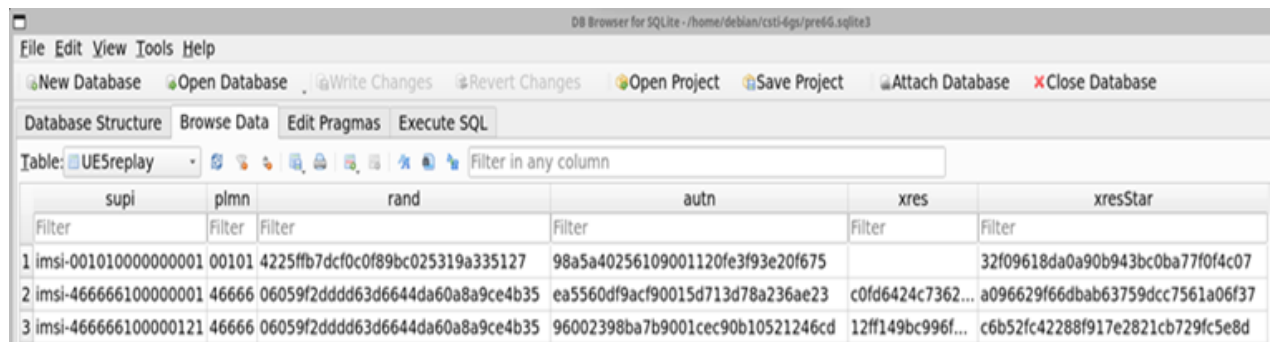


圖 114、Pre-6G 假核心網路與 gNB 跳脫認證程序安全威脅-誘騙攻擊

資料來源：本計畫整理

(3)透過網路分析器 (Sniffer) 獲得認證向量儲存在假統一資料管理功能的重播認證向量資料庫中，如圖 115 所

示，分析器(Sniffer)獲得認證向量包括 SUPI、PLMN、rand、autn、xres、xresStar (xres*)等參數。



	supi	plmn	rand	autn	xres	xresStar
1	imsi-001010000000001	00101	4225fb7dcf0c0f89bc025319a335127	98a5a40256109001120fe3f93e20f675		32f09618da0a90b943bc0ba77f0f4c07
2	imsi-466666100000001	46666	06059f2ddd63d6644da60a8a9ce4b35	ea5560df9ac90015d713d78a236ae23	c0fd6424c7362...	a096629f66dbab63759dcc7561a06f37
3	imsi-466666100000121	46666	06059f2ddd63d6644da60a8a9ce4b35	96002398ba7b9001cec90b10521246cd	12ff149bc996f...	c6b52fc42288f917e2821cb729fc5e8d

圖 115、假統一資料管理功能重播認證向量資料庫

資料來源：本計畫整理

(二)假用戶對核網的攻擊

模擬 6G 跨領域應用環境，用戶端攻擊者藉由發送假網路封包資料，鎖定網路系統漏洞或是協定機制的缺陷進行攻擊，藉由伺服器須處理此些封包回應而無法用於合法流量，目的是讓網路系統的功能癱瘓或資源耗盡。

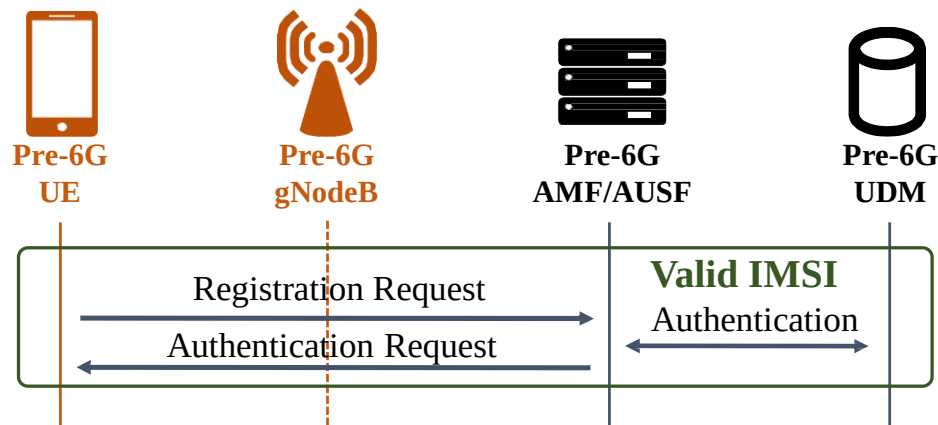
1. Pre-6G 核心網路 SUPI 帳號填充攻擊

(1)帳號填充攻擊是一種以自動化方式，不斷使用有規則的憑證序號或偷來的登入憑證，試圖登入網路服務的一種攻擊技巧。這項手法使用大量的憑證再搭配自動化腳本，以疲勞轟炸的方式不斷試圖登入網路服務，直到某一組帳號密碼成功為止。

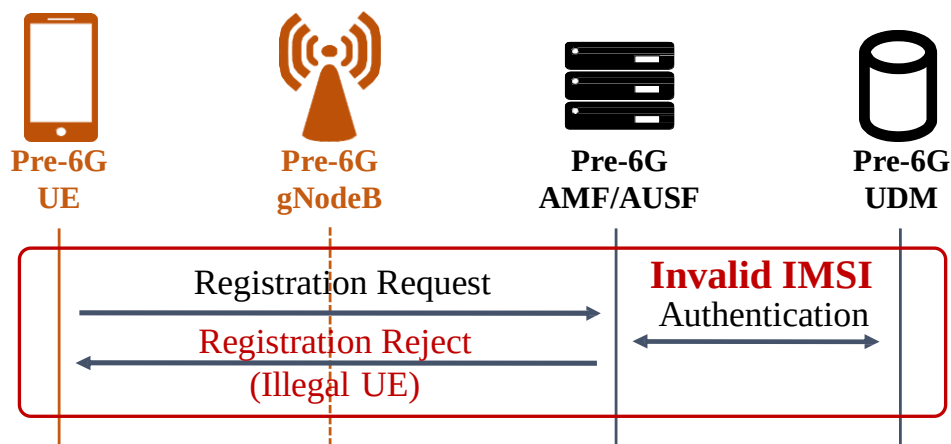
(2)SUPI 或 IMSI 是區別行動裝置用戶的標誌，儲存在 SIM 卡中，可用於區別行動裝置用戶的有效訊息，在所有蜂巢式網路中不重複辨識碼，有效的識別碼(Valid IMSI)在傳輸給 gNB 時會快速驗證 IMSI 號碼的狀態而給予回應，相對的無效識別碼(Invalid IMSI)則不會得到任何回應，惡意攻擊者可使用 gNB 這個機制，大

量模擬 IMSI 號碼，取得有效與無效的識別碼進行下一步攻擊準備。

(3)本計畫實作終端用戶對 Pre-6G 核心網路進行 SUPI 帳號填充攻擊，透過該攻擊測試取得合法的 SUPI 清單。由於該項實驗是終端用戶，透過 NAS 直接對 Pre-6G 核心網路進行帳號填充攻擊，故本實驗直接透過 N2 介面來實測驗證系統架構示意圖，如圖 116 所示。



(a)有效識別碼(Valid identity)



(b)無效識別碼(Invalid identity)

圖 116、Pre-6GC 核心網路 SUPI 帳號填充攻擊實驗架構

資料來源：本計畫整理

(4)本計畫團隊透過自行開發的 Pre-6G gNB 與 UE 模擬器，NAS 直接對 Pre-6G 核心網路進行帳號填充攻擊，

實現 Pre-6G 核心網路用戶 SUPI 帳號填充攻擊實測驗證，如圖 117 所示。



圖 117、Pre-6G 核心網路用戶 SUPI 帳號填充攻擊實測驗證

資料來源：本計畫整理

2. Pre-6G AMF 的 N1 介面攻擊測試

(1) 本計畫實作終端用戶對 Pre-6G 核心網路進行的 N1 介面攻擊，透過該攻擊測試確認 AMF 的資安防護是否符合標準規範，測試項目由本團隊與耀睿科技 OTIC 實驗室依據 O-RAN Alliance Working Group 11(WG11) 正在討論的開放架構資訊安全議題，設計涵蓋 8 個攻擊情境如表 40。

表 40、Pre-6G AMF 的 N1 介面攻擊測試項目

編號	測試項目	攻擊測試目的
4.2.2.1.1	Synchronization failure handling	驗證 AMF 中的安全錨定功能(Security Anchor Function, SEAF)是否正確處理同步失敗。
4.2.2.1.2	RES* verification failure handling	驗證 AMF 中的 SEAF 是否正確處理 RES *驗證失敗。
4.2.2.3.1	Replay protection of NAS signalling messages	驗證 AMF 的 N1 介面上 NAS 訊令受到重播保護。
4.2.2.3.2	NAS NULL integrity protection	驗證只有緊急電話才能於 NAS 使用無完整性保護演算法(NULL integrity protection algorithm)。
4.2.2.3.3	NAS integrity algorithm selection and use	AMF 依據其非存取層完整性保護演算法(NAS integrity algorithm)優先順序設定以及 UE 安全能力(UE security capability)，選擇完整性保護演算法優先順序以及中最高優先權(Highest Priority)之設定。
4.2.2.4.1	Bidding down prevention in Xn-handover	驗證當 Xn 換手時發生降級(Bidding Down)攻擊時，AMF 會保留記錄。
4.2.2.5.1	5G-GUTI allocation	AMF 在以 Initial Registration 或 Mobility Registration Update 方式重新入網註冊後會配置新的 5G-GUTI。
4.2.2.6.1	Invalid or unacceptable UE security capabilities handling	AMF 不接受不支援任何完整性保護與加密演算法的 UE 安全設定。

資料來源：本計畫整理

(2)由於該項實驗是終端用戶透過 NAS 直接對 Pre-6G 核心網路 N1 介面攻擊，故本實驗直接透過 N2 介面來實測驗證，系統架構示意圖，如圖 118 所示。

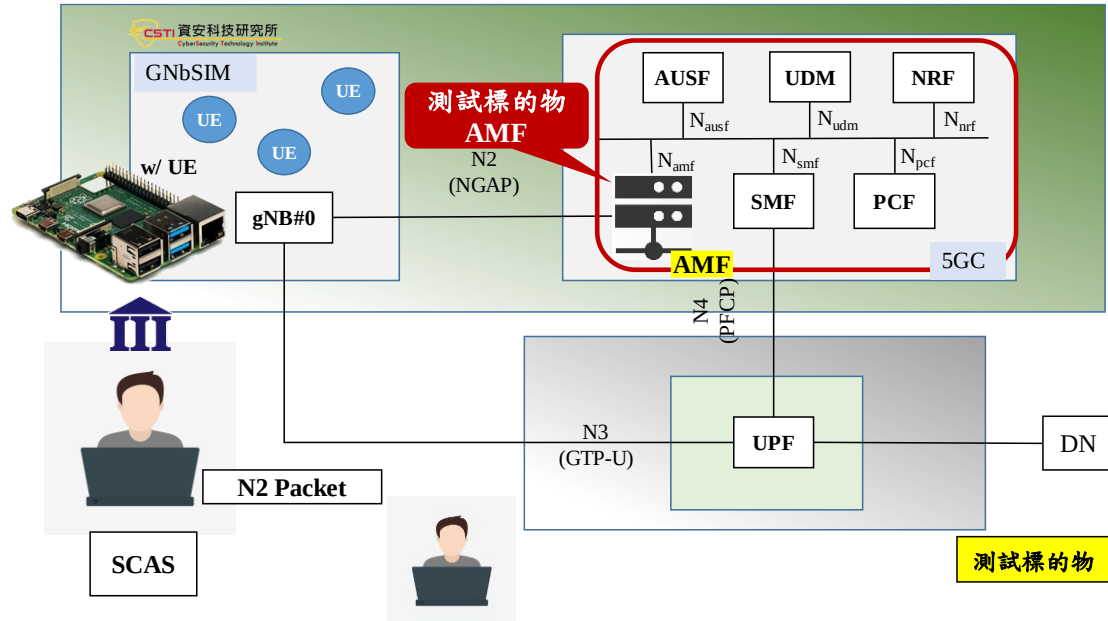


圖 118、Pre-6G AMF 的 N1 介面攻擊測試實驗架構

資料來源：本計畫整理

(3)本計畫 Pre-6G AMF 的 N1 介面攻擊之測試方法與步驟如表 41 至表 48 所示。

表 41、Synchronization failure handling

編號	4.2.2.1.1	標的	Pre-6G AMF
檢測項目	Synchronization failure handling		
測試步驟	1. 用戶設備(UE)向 AMF 中的 SEAF 發送夾帶同步失敗(AUTS)的驗證失敗(Authentication Failure)訊息。 2. AMF 中的 SEAF 向 UE 發送夾帶認證資訊(AUTN)的驗證請求(Authentication Request)訊息。 3. UE 向 AMF 中的 SEAF 成功發送驗證回應(Authentication Response)訊息。		

資料來源：本計畫整理

表 42、RES* verification failure handling

編號	4.2.2.1.2	標的	Pre-6G AMF
檢測項目	RES* verification failure handling		
測試步驟	1. UE 向 AMF 中的 SEAF 傳送夾帶不正確 RES*數值的 NAS Authentication Response 訊息。 2. AMF 中的 SEAF 從 RES*數值計算出 HRES*數值，並比對 HRES*與 HXRES*數值使否相同。 3. AMF 中的 SEAF 向 UE 發送驗證拒絕(Authentication Reject)訊息。		

資料來源：本計畫整理

表 43、Replay protection of NAS signalling messages

編號	4.2.2.3.1	標的	Pre-6G AMF
檢測項目	Replay protection of NAS signalling messages		
測試步驟	1. UE 向 AMF 傳送安全模式完成(Security Mode Complete)訊息。 2. AMF 向 UE 發送接受註冊(Registration Accept)訊息。 3. UE 向 AMF 傳送相同的 Security Mode Complete 訊息。 4. AMF 不會向 UE 發送任何訊息。		

資料來源：本計畫整理

表 44、NAS NULL integrity protection

編號	4.2.2.3.2	標的	Pre-6G AMF
檢測項目	NAS NULL integrity protection		
測試步驟	1. UE 向 AMF 傳送夾帶只允許 EIA0 (5G-IA0)的註冊請求(Registration Request)訊息。 2. AMF 應該向 UE 發送拒絕註冊(Registration Reject)訊息。但 AMF 實際上向 UE 發送夾帶使用無完整性保護演算法(NULL Integrity Protection Algorithm) 的安全模式指令(Security Mode Command) 訊息。		

資料來源：本計畫整理

表 45、NAS integrity algorithm selection and use

編號	4.2.2.3.3	標的	Pre-6G AMF
檢測項目	NAS integrity algorithm selection and use		
測試步驟	AMF 依據其 NAS integrity algorithm 優先順序設定為 EIA2 (128-5G-IA2) → EIA1 (128-5G-IA1)。 1. UE 向 AMF 傳送夾帶只允許 EIA1 (128-5G-IA1) 的 Registration Request 訊息。 2. AMF 向 UE 發送夾帶使用 EIA1 (128-5G-IA1) 的 Security Mode Command 訊息。 3. UE 向 AMF 傳送夾帶只允許 EIA2 (128-5G-IA2) 的 Registration Request 訊息。 4. AMF 向 UE 發送夾帶使用 EIA2 (128-5G-IA2) 的 Security Mode Command 訊息。		

資料來源：本計畫整理

表 46、Bidding down prevention in Xn-handover

編號	4.2.2.4.1	標的	Pre-6G AMF
檢測項目	Bidding down prevention in Xn-handover		
測試步驟	1. 目標 5G 基地臺(target gNB)向存取與行動管理功能(AMF)傳送夾帶竄改過的用戶設備安全能力(UE security capability)的 Path-Switch Request 訊息。 2. 存取與行動管理功能(AMF)應該向目標 5G 基地臺(target gNB)傳送夾帶竄改前的用戶設備安全能力(UE security capability)的 Path-Switch Request Acknowledge 訊息，同時保留記錄。		

資料來源：本計畫整理

表 47、5G-GUTI allocation

編號	4.2.2.5.1	標的	Pre-6G AMF
檢測項目	5G-GUTI allocation		
測試步驟	1. 用戶設備(UE)向存取與行動管理功能(AMF)傳送夾帶 Initial Registration 及 5G-GUTI 的 Registration Request 訊息。 2. 存取與行動管理功能(AMF)向用戶設備(UE)發送夾帶更新 5G-GUTI 的 Registration Accept 訊息。 3. 用戶設備(UE)向存取與行動管理功能(AMF)傳送夾帶 Mobility Registration Update 及 5G-GUTI 的 Registration Request 訊息。 4. 存取與行動管理功能(AMF)向用戶設備(UE)發送夾帶更新 5G-GUTI 的 Registration Accept 訊息。		

資料來源：本計畫整理

表 48、Invalid or unacceptable UE security capabilities handling

編號	4.2.2.6.1	標的	Pre-6G AMF
檢測項目	Invalid or unacceptable UE security capabilities handling		
測試步驟	1. 用戶設備(UE)向存取與行動管理功能(AMF)傳送夾帶不支援任何完整性保護與加密演算法的 Registration Request 訊息。 2. 存取與行動管理功能(AMF)向用戶設備(UE)發送 Registration Reject 訊息。		

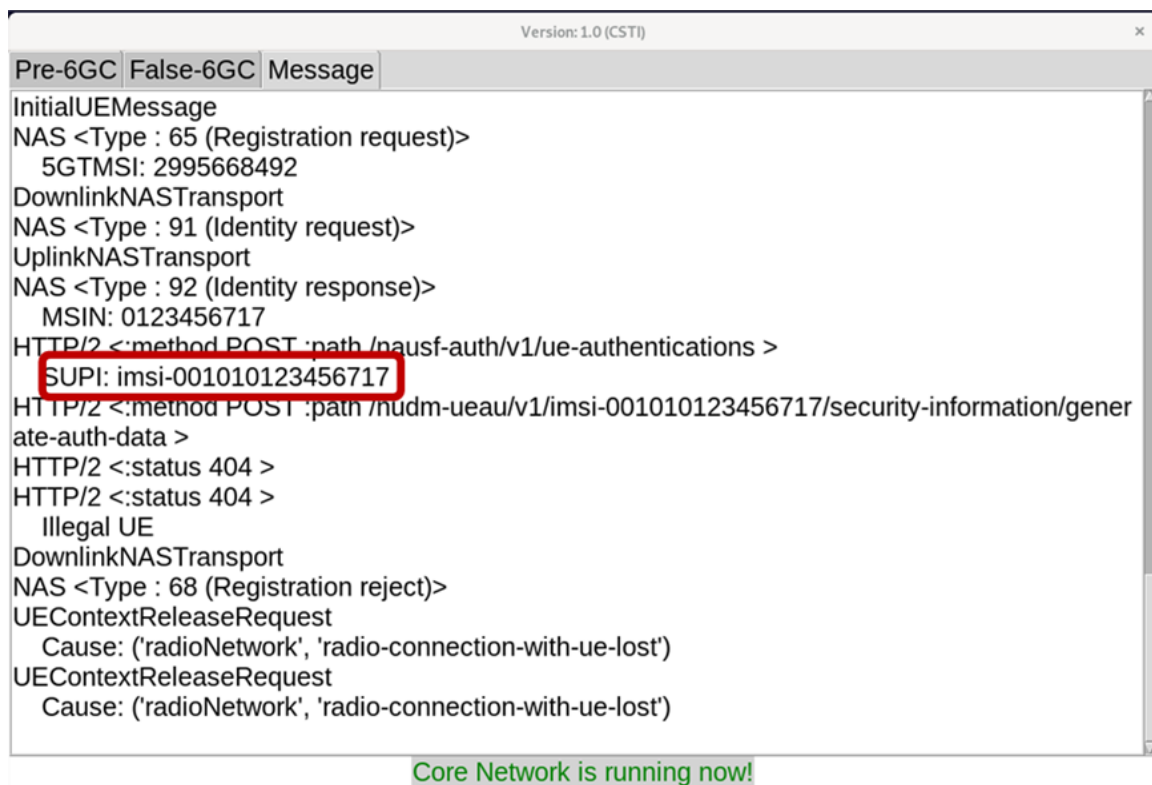
資料來源：本計畫整理

七、測試數據與測試結果之探討

(一)假核網+基地臺誘騙用戶攻擊

1. 「Pre-6G SUPI/IMSI 捕捉器與入網阻斷服務攻擊」測試數據

SUPI/IMSI 捕捉器利用假基地臺裝置對 UE 實現捕捉 UE 的 SUPI，如圖 119 所示。緊接著，Pre-6G 核心網路模擬器透過回復夾帶原因(Cause)為 Illegal UE 的拒絕註冊(Registration Reject)訊令，達成用戶對 DoS 的攻擊，如圖 120 所示。



```
Version: 1.0 (CSTI)
Pre-6GC False-6GC Message
InitialUEMessage
NAS <Type : 65 (Registration request)>
  5GTMSI: 2995668492
DownlinkNASTransport
NAS <Type : 91 (Identity request)>
UplinkNASTransport
NAS <Type : 92 (Identity response)>
  MSIN: 0123456717
HTTP/2 <:method POST :path /nausf-auth/v1/ue-authentications >
  SUPI: imsi-001010123456717
HTTP/2 <:method POST :path /nudm-ueau/v1/imsi-001010123456717/security-information/generate-auth-data >
HTTP/2 <:status 404 >
HTTP/2 <:status 404 >
  Illegal UE
DownlinkNASTransport
NAS <Type : 68 (Registration reject)>
UEContextReleaseRequest
  Cause: ('radioNetwork', 'radio-connection-with-ue-lost')
UEContextReleaseRequest
  Cause: ('radioNetwork', 'radio-connection-with-ue-lost')
Core Network is running now!
```

圖 119、Pre-6G SUPI/IMSI 捕捉器擷取竊聽用戶的實測驗證

資料來源：本計畫整理

No.	Time	Source	Destination	Protocol	Length	Seq	Info
9...	192.168.1.33	192.168.1.100	NGAP	124			NGSetupRequest
9...	192.168.1.100	192.168.1.33	NGAP	120			NGSetupResponse
15...	192.168.1.33	192.168.1.100	NGAP/...	204			InitialUEMessage, Registration request, Registration request
15...	192.168.1.100	192.168.1.33	NGAP/...	108			SACK (Ack=1, Arwnd=106496), DownlinkNASTransport, Identity request
15...	192.168.1.33	192.168.1.100	NGAP/...	148			SACK (Ack=1, Arwnd=106496), UplinkNASTransport, Identity response
15...	192.168.1.100	192.168.1.33	NGAP/...	108			SACK (Ack=2, Arwnd=106496), DownlinkNASTransport, Registration reject (Illegal
25...	192.168.1.33	192.168.1.100	NGAP	92			UEContextReleaseRequest


```

value
  RAN-UE-NGAP-ID: 2
Item 2: id-NAS-PDU
  ProtocolIE-Field
    id: id-NAS-PDU (38)
    criticality: reject (0)
  value
    NAS-PDU: 7e004403
      Non-Access-Stratum 5GS (NAS)PDU
        Plain NAS 5GS Message
          Extended protocol discriminator: 5G mobility management messages (126)
          0000 .... = Spare Half Octet: 0
          .... 0000 = Security header type: Plain NAS message, not security protected (0)
          Message type: Registration reject (0x44)
          5GMM cause
            5GMM cause: Illegal UE (3)

```

圖 120、夾帶 Cause(Illegal UE)的拒絕註冊訊令

資料來源：本計畫整理

2. 「Pre-6G 假核心網路與 gNB 誘騙攻擊」測試數據

Amarisoft 的軟體 UE 設定設為支援 5G-IA0，在接收到安全模式設定夾帶 Null Security 的訊令後，規避加密與完整性檢查並達成後續的入網程序，如圖 121 與圖 122 所示。

Replay Authentication Vector

Source	Destination	Protocol	Length	Info
192.168.1.6	192.168.1.80	NGAP/NAS-5GS	146	DownlinkNASTransport, Authentication request
192.168.1.80	192.168.1.6	NGAP/NAS-5GS	142	UplinkNASTransport, Authentication response


```

Plain NAS 5GS Message
  Extended protocol discriminator: 5G mobility management messages (126)
  0000 .... = Spare Half Octet: 0
  .... 0000 = Security header type: Plain NAS message, not security protected (0)
  Message type: Authentication request (0x56)
  0000 .... = Spare Half Octet: 0
  NAS key set identifier - ngKSI
  ABBA
  Authentication Parameter RAND - 5G authentication challenge
    Element ID: 0x21
    RAND value: 06059f2ddddd63d6644da60a8a9ce4b35
  Authentication Parameter AUTN (UMTS and EPS authentication challenge) - 5G authentication challenge
    Element ID: 0x20
    Length: 16
    AUTN value: ea5560df9acf90015d713d78a236ae23
      SQN xor AK: ea5560df9acf
      AMF: 9001
      MAC: 5d713d78a236ae23

```

重播網路分析器獲得的認證向量

Amarisoft與NemoHandy用戶終端都會發送Authentication Response，並通過認證

圖 121、Pre-6G 假核心網路與 gNB 重播 AV 的實測驗證

資料來源：本計畫整理



圖 122、Amarisoft 的軟體 UE 的實測驗證

資料來源：本計畫整理

Nemo Handy 將 UE 安全設定設為不支援 5G-IA0，以防止安全模式設中發送 Null Security 的方式避免遭受誘騙，如圖 123 與圖 124 所示。

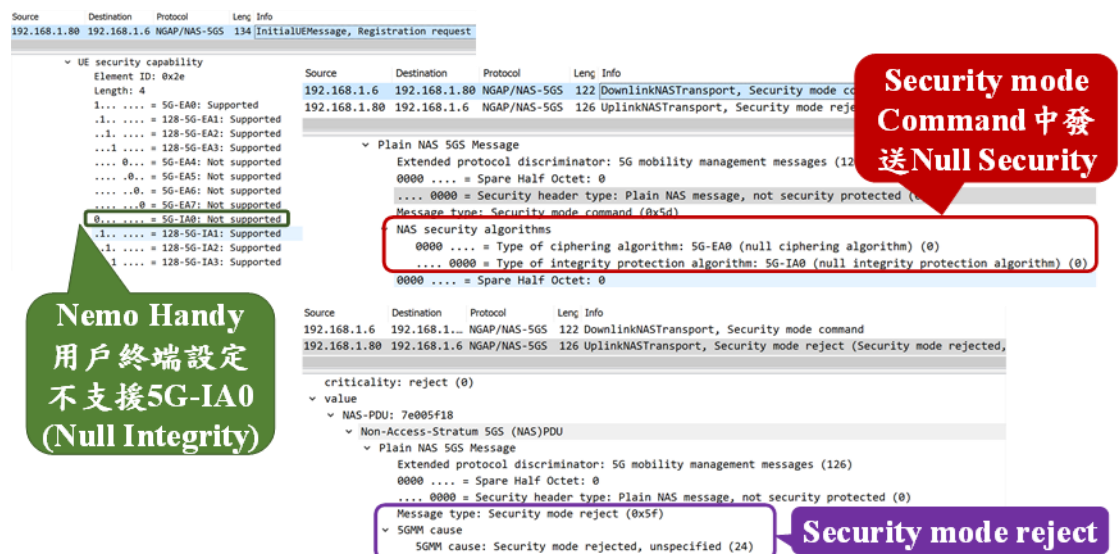


圖 123、Nemo Handy 的實測驗證

資料來源：本計畫整理

Source	Destination	Protocol	Length	Info
192.168.1.80	192.168.1.6	NGAP/NAS-5GS	134	InitialUEMessage, Registration request
192.168.1.6	192.168.1.80	NGAP/NAS-5GS	118	DownlinkNASTransport, Security mode command
192.168.1.80	192.168.1.6	NGAP/NAS-5GS	146	UplinkNASTransport, Security mode complete
192.168.1.6	192.168.1.80	NGAP/NAS-5GS	222	InitialContextSetupRequest, Registration accept
192.168.1.80	192.168.1.6	NGAP	158	UERadioCapabilityInfoIndication
192.168.1.80	192.168.1.6	NGAP	82	InitialContextSetupResponse
192.168.1.80	192.168.1.6	NGAP/NAS-5GS	118	UplinkNASTransport, Registration complete

Pre-6G UE順利完成註冊

Pre-6G AMF在收到Pre-6G UE的Registration request後Pre-6G UE發送Security Command

Security mode Command中發送Null Security

```

NAS-PDU: 7e03000000000000
├─ Non-Access-Stratum 5GS (NAS)PDU
│   └─ Security protected NAS 5GS message
│       └─ Plain NAS 5GS Message
│           Extended protocol discriminator: 5G mobility management messages (126)
│           0000 .... = Spare Half Octet: 0
│           .... 0000 = Security header type: Plain NAS message, not security protected
│           Message type: Security mode command (0x5d)
│           └─ NAS security algorithms
│               0000 .... = Type of ciphering algorithm: 5G-EA0 (null ciphering algorithm) (0)
│               .... 0000 = Type of integrity protection algorithm: 5G-IA0 (null integrity protection algorithm) (0)
│               0000 .... = Spare Half Octet: 0

```

圖 124、Amarisoft 的軟體 UE 的實測驗證

資料來源：本計畫整理

3. 「假核網+基地臺誘騙用戶攻擊」測試結果探討

依據測試結果得出的結論，既有的電信系統的廣播訊號缺乏合法電信事業身分的確認機制，所以 UE 無法確認廣播電信訊號是否為合法電信系統發送，導致 UE 不慎嘗試連接非法的電信網系統，致使 UE 的身分機敏資料(SUPI/IMSI)外洩與 UE 所在位置被利用。

用戶對 DoS 攻擊，建議緩解措施為加入合法電信事業身分確認機制，需要透過修改 3GPP 標準文件強化防範，目前 Apple 在 3GPP 標準委員會提案解決這個議題。

在面對假核心網路與 gNB 誘騙攻擊之緩解措施為禁止 UE 支援 Null Security 的設定。將 UE 安全設定設為不支援 5G-IA0，以防止 SMC 發送 Null Security 的方式避免遭受誘騙。

(二)假終端用戶攻擊核網+基地臺

1. 「Pre-6G 核心網路 SUPI 帳號填充攻擊」測試數據

Pre-6G gNB 與 UE 模擬器透過 NAS 直接對 Pre-6G 核心網路進行帳號填充攻擊，成功獲得有效識別碼(Valid identity)與無效識別碼(Invalid identity)清單，如圖 125 所示。

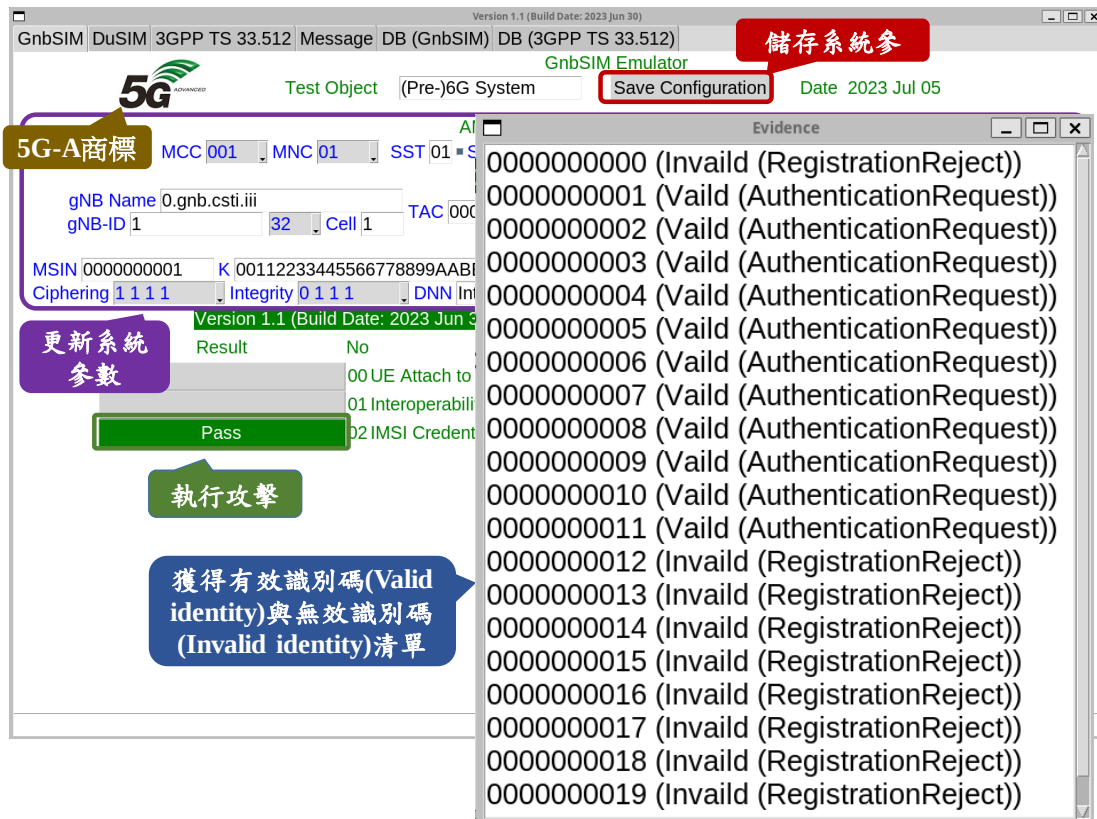


圖 125、Pre-6GC 核心網路 SUPI 帳號填充攻擊器操作介面

資料來源：本計畫整理

2. 「Pre-6G AMF 的 N1 介面攻擊測試」測試數據

Pre-6G AMF 的 N1 介面攻擊之測試操作介面如圖 126 所示，對 Amarisoft 軟體核心網路攻擊測試數據結果整理為表 49，依據 N1 介面攻擊之測試方法與步驟的測試證據如圖 127 至圖 134 所示：

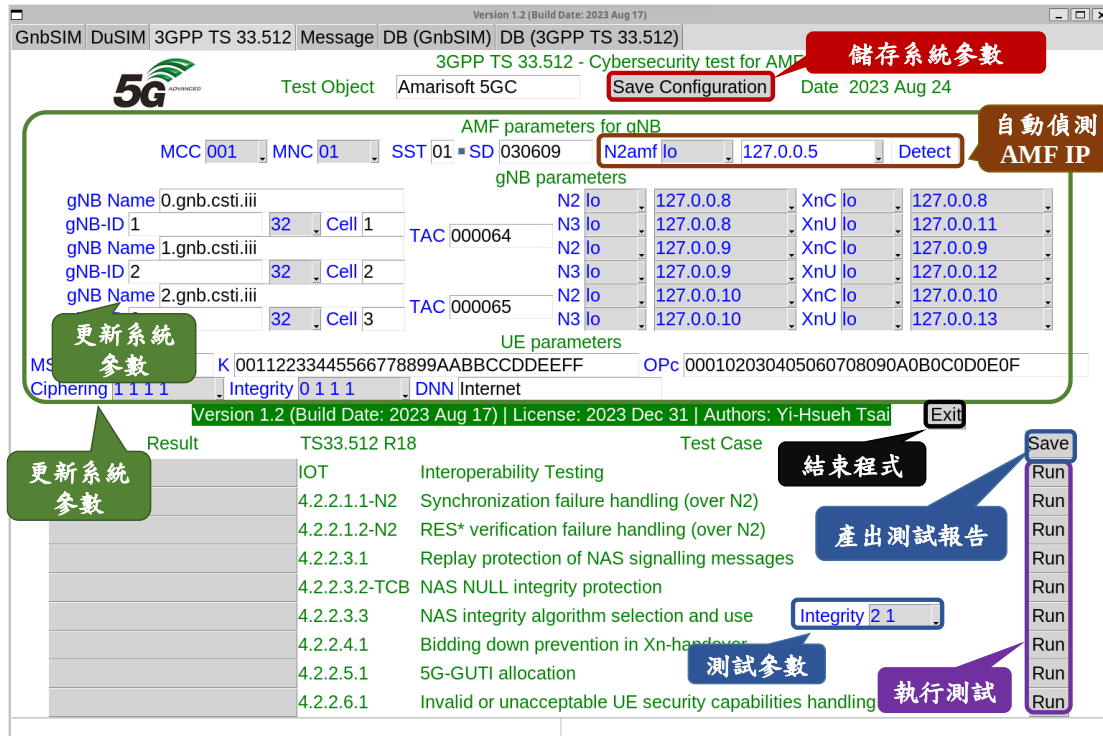


圖 126、Pre-6G AMF 的 N1 介面攻擊測試器操作介面

資料來源：本計畫整理

本次測試實證是依據 3GPP R17 完成 5G 通訊基本架構，在此基礎上參考 3GPP 最新研議 R18 技術標準(審議中版本，尚未成為正式標準)，試做無線接取基地臺強化動態頻譜分享功能，開發支持最新版本 Amarisoft 模擬器 AMF 網路元件與介面，以現行 3GPP SCAS TS33.512 安全標準的 8 個測項進行安全檢測：(1)測試結果「PASS」判讀為尚能符合現行的資安標準；(2)「Fail」則是不符合現行安全標準規範或是未有資料產出而無法判讀。下表分析此次實證的測試結果，有 3 個測項「Fail」皆屬 R18 新介面，無法依循現有的標準判讀，須待進一步增修新版本的國際通訊安全標準。

表 49、「Pre-6G AMF 的 N1 介面攻擊」測試結果

No.	Test Object	Test Item	Result
01	Amarisoft's AMF	Synchronization failure handling (over N2)	Pass
02	Amarisoft's AMF	RES* verification failure handling (over N2)	Pass
03	Amarisoft's AMF	Replay protection of NAS signalling messages	Pass
04	Amarisoft's AMF	NAS NULL integrity protection	Fail
05	Amarisoft's AMF	NAS integrity algorithm selection and use	Pass
06	Amarisoft's AMF	Bidding down prevention in Xn-handover	Fail
07	Amarisoft's AMF	5G-GUTI allocation	Pass
08	Amarisoft's AMF	Invalid or unacceptable UE security capabilities handling	Fail

資料來源：本計畫整理

Evidence	<<<TS 33.512 5G SCAS; AMF - Section 4.2.2.1.1 Synchronization failure handling (over N2)>>> NAS Message Type: <Type : 89 (Authenticion failure)> Step 1: Check NAS Authenticion failure 5GMM Cause: <5GMMCause : 21 (Synch failure)> AUTS: d7aab5552ac2213ffdc042c9289 Step 1: Pass NAS Message Type: <Type : 66 (Registration accept)> Step 2: Check NAS Registration accept AUTH counter: 2 Step 2: Pass Pass Test Case

圖 127、Synchronization failure handling (over N2) 測試

資料來源：本計畫整理

Evidence	<<<TS 33.512 5G SCAS; AMF - Section 4.2.2.1.2 RES* verification failure handling>>> NAS Message Type: <Type : 87 (Authentication response)> Step 1: Check NAS Authentication response AUTS: 7ffb9280d9f0bf1d2065c6c99c332bc2 Step 1: Pass NAS Message Type: <Type : 88 (Authentication reject)> Step 2: Check NAS Authentication reject Step 2: Pass Pass Test Case

圖 128、RES* verification failure handling (over N2)測試

資料來源：本計畫整理

Evidence	<<<TS 33.512 5G SCAS; AMF - Section 4.2.2.3.1 Replay protection of NAS signalling messages>>> NAS Message Type: <Type : 93 (Security mode command)> Step 1: Check NAS Security mode command Selected NAS integrity algorithm: 2 UE integrity capabilities: NIA0: 0, NIA1: 1, NIA2: 1, NIA3: 0 Step 1: Pass NAS Message Type: <Type : 66 (Registration accept)> Step 2: Check NAS Registration accept Step 2: Pass NAS Message Type: <Type : 104 (DL NAS transport)> Step 3: Check replay protection counter of NAS Registration accept: 1 Step 3: Pass Pass Test Case

圖 129、Replay protection of NAS signalling messages 測試

資料來源：本計畫整理

Evidence

<<<TS 33.512 5G SCAS; AMF - Section 4.2.2.3.2 NAS NULL integrity protection>>>

NAS Message Type: <Type : 93 (Security mode command)>**Step 1: Check NULL integrity protection****Selected NAS integrity algorithm:** 0**UE integrity capabilities:** NIA0: 1, NIA1: 0, NIA2: 0, NIA3: 0**Step 1: Fail****Fail Test Case****NAS Message Type:** <Type : 93 (Security mode command)>**Step 1: Check NULL integrity protection****Selected NAS integrity algorithm:** 2**UE integrity capabilities:** NIA0: 0, NIA1: 1, NIA2: 1, NIA3: 0**Step 1: Pass****Pass Test Case**

圖 130、NAS NULL integrity protection 測試

資料來源：本計畫整理

Evidence

<<<TS 33.512 5G SCAS; AMF - Section 4.2.2.3.3 NAS integrity algorithm selection and use>>>

NAS Message Type: <Type : 66 (Registration accept)>**Step 1: Check ordered lists of NAS integrity algorithm****Ordered lists of NAS integrity algorithm:** [2, 1]**Selected NAS integrity algorithm:** 1**UE integrity capabilities:** NIA0: 0, NIA1: 1, NIA2: 0, NIA3: 0**Step 1: Pass****Pass Test Case****NAS Message Type:** <Type : 66 (Registration accept)>**Step 1: Check ordered lists of NAS integrity algorithm****Ordered lists of NAS integrity algorithm:** [2, 1]**Selected NAS integrity algorithm:** 2**UE integrity capabilities:** NIA0: 0, NIA1: 0, NIA2: 1, NIA3: 0**Step 1: Pass****Pass Test Case****NAS Message Type:** <Type : 66 (Registration accept)>**Step 1: Check ordered lists of NAS integrity algorithm****Ordered lists of NAS integrity algorithm:** [2, 1]**Selected NAS integrity algorithm:** 0**UE integrity capabilities:** NIA0: 0, NIA1: 0, NIA2: 0, NIA3: 1**Step 1: Pass****Pass Test Case**

圖 131、NAS integrity algorithm selection and use 測試

資料來源：本計畫整理

Evidence

<<<TS 33.512 5G SCAS; AMF - Section 4.2.2.4.1 Bidding down prevention in Xn-handover>>>

NAS Message Type: <Type : 104 (DL NAS transport)>

Step 1: Check UE Security Capabilities in Handover Request:

nRencryptionAlgorithms: NEA1: False, NEA2: False, NEA3: False

nRintegrityProtectionAlgorithms: NIA1: True, NIA2: True, NIA3: False

Step 1: Pass

NAS Message Type: <Type : 104 (DL NAS transport)>

Step 2: Check Mismatch UE Security Capabilities in Handover Request:

nRencryptionAlgorithms: NEA1: False, NEA2: False, NEA3: False

nRintegrityProtectionAlgorithms: NIA1: False, NIA2: False, NIA3: False

Step2: Pass

NAS Message Type: <Type : 104 (DL NAS transport)>

Step 3: Check UE Security Capabilities in Path Switch Request:

nRencryptionAlgorithms: NEA1: False, NEA2: False, NEA3: False

nRintegrityProtectionAlgorithms: NIA1: True, NIA2: True, NIA3: False

New Security Context Indication: False

Step 3: Fail

Fail Test Case

圖 132、Bidding down prevention in Xn-handover 測試

資料來源：本計畫整理



Evidence	<<<TS 33.512 5G SCAS; AMF - Section 4.2.2.5.1 5G-GUTI allocation>>> NAS Message Type: <Type : 65 (Registration request)> Step 1: Check Registration Type and 5GSID 5GS RegType: <Value : 1 (initial registration)> SUCI: <PLMN : 00101> <Output : 0 -> MSIN : 0000000001> Step 1: Pass NAS Message Type: <Type : 66 (Registration accept)> Step 2: Compare old GUTI and new GUTI GUTI: <GUTI : <T : 119><L : 11><5GSID : <ind : 0xf><spare : 0><Type : 2 (5G-GUTI)><PLMN : 00101><AMFRegionID : 128><AMFSetID : 4><AMFPtr : 1><5GTMSI : 0xafb42fb6>>> Step 2: Pass Pass Test Case NAS Message Type: <Type : 65 (Registration request)> Step 1: Check Registration Type and 5GSID 5GS RegType: <Value : 1 (initial registration)> TMSI: 2947821494 Step 1: Pass NAS Message Type: <Type : 66 (Registration accept)> Step 2: Compare old GUTI and new GUTI GUTI: <GUTI : <T : 119><L : 11><5GSID : <ind : 0xf><spare : 0><Type : 2 (5G-GUTI)><PLMN : 00101><AMFRegionID : 128><AMFSetID : 4><AMFPtr : 1><5GTMSI : 0xa06c22f8>>> Step 2: Pass Pass Test Case NAS Message Type: <Type : 65 (Registration request)> Step 1: Check Registration Type and 5GSID 5GS RegType: <Value : 2 (mobility registration updating)> TMSI: 2691441400 Step 1: Pass NAS Message Type: <Type : 66 (Registration accept)> Step 2: Compare old GUTI and new GUTI GUTI: <GUTI : <T : 119><L : 11><5GSID : <ind : 0xf><spare : 0><Type : 2 (5G-GUTI)><PLMN : 00101><AMFRegionID : 128><AMFSetID : 4><AMFPtr : 1><5GTMSI : 0xf2e2a983>>> Step 2: Pass Pass Test Case

圖 133、5G-GUTI allocation 測試

資料來源：本計畫整理

Evidence	<<<TS 33.512 5G SCAS; AMF - Section 4.2.2.6.1 Invalid or unacceptable UE security capabilities handling>>> NAS Message Type: <Type : 65 (Registration request)> Step 1: Check UE Security Capabilities UE security capabilities: NIA0: 0, NIA1: 0, NIA2: 0, NIA3: 0 UE encryption capabilities: NEA0: 0, NEA1: 0, NEA2: 0, NEA3: 0 Step 1: Pass NAS Message Type: <Type : 93 (Security mode command)> Step 2: Check Selected Security algorithms Selected NAS integrity algorithm: 0 Selected NAS encryption algorithm: 0 Step 2: Pass NAS Message Type: <Type : 66 (Registration accept)> Step 3: Check Registration evidence for NULL Security Step 3: Fail Fail Test Case

圖 134、Invalid or unacceptable UE security capabilities handling 測試

資料來源：本計畫整理

3. 「假用戶對核網的攻擊」測試結果探討

對於 SUPI 帳號填充攻擊，建議緩解為一律要求 UE 進行入網身分認證。無論 UE 的識別碼有效與否，核網與基站一律要求 UE 進行完整身分驗證入網流程，避免攻擊者透過入網流程，列舉系統中有效的識別碼，做為後續攻擊可利用資訊，則需要透過修改 3GPP 標準文件才能徹底防範。

Pre-6G AMF 的 N1 介面攻擊測試，牽涉到網通產品的開發從需求、設計、開發到測試，把資安元素放入初始程式開發流程，透過 3GPP 創建的 SCAS，GSMA 則制定認證流程、產品開發過程的安全性審核，以及測試實驗室資質相關的 NESAS，確保落實 6G 核心網路通訊安全測試評估，確保



6G 系統架構做到預設安全(Security By Design)不僅只是網路安全防護的管理，更將資安納入軟體產品開發端。

上述 Pre-6G 防護實證的結果，本團隊已將「Pre-6G AMF 的 N1 介面攻擊測試」8 個測試項目之測試方法、步驟與結果，與國際 O-RAN 聯盟認證之耀睿 OTIC 實驗室討論，將目前已發現的資安議題，於耀睿實驗室提供 5G O-RAN 的資安檢測服務同時考量進去，輔助國內 5G 網通設備廠商投入實際應用；耀睿亦可於檢測服務過程中取得測試結果數據做為佐證，在參加 O-RAN 聯盟 SFG 安全焦點群組 (Security Focus Group) 技術討論會議時，回饋國內 Pre-6G 相關資安技術的前期研究與測試結果，促進 O-RAN 聯盟於未來 Pre-6G 安全技術議題，制定與 3GPP 規範一致的 O-RAN 安全規範，形成國內外技術同步的正向循環。

第四節 6G 資安產業研析座談會

隨著連網設備增加，駭客的攻擊入口就愈多，網路安全和隱私問題突顯其重要性，資安風險緩解應該成為 IoT 架構的組成部分，5G 通訊技術實現萬 IoT 的應用，未來 5 年可望成為 IoT 支出金額年成長最高的產業，大量 UE 或傳感設備連接在 IoT 中，可實現具備社會、工業和商業用例的即時通訊系統，藉由探討通訊 IoT 應用之系統架構，涵蓋傳輸層、應用層及資料層之網路安全技術發展趨勢，參酌國際發展經驗及前揭蒐集資料，辦理座談會議至少 4 場次，邀請討論議題之相關利害關係者(共計 50 家廠商以上之出席)，蒐集國內現況及產官學等意見。

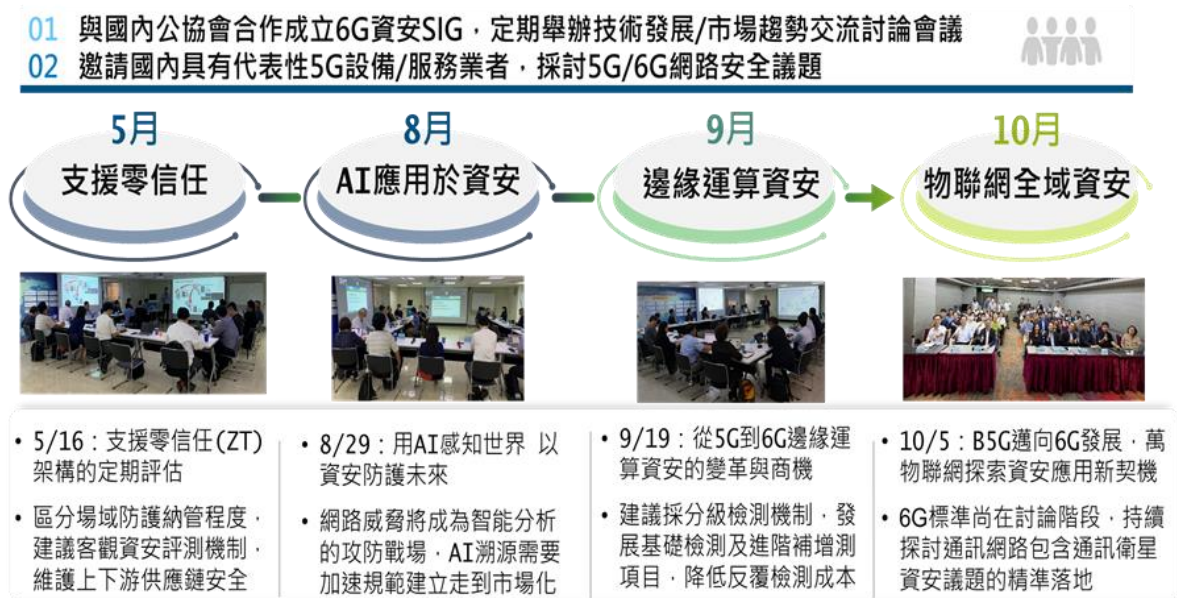


圖 135、6G 資安產業研析 4 場座談會彙整

資料來源：本計畫整理

本計畫 6G 資安產業研析座談會詳細內容，請參閱附件 2。

藉助國內台灣雲端物聯網產業協會已成立物聯網資安 SIG，與公協會會員廠商策略合作，於下半年針對未來 6G 資安防護/防護對應生態辦理至少 3 場次活動(包括 6G 資安趨勢探討座談會 3 場次、推廣活動 1 場次)，持續與國內 5G/6G 產研專家與對應產業關鍵成員，共

同擘劃多元、創新 5G 到 Pre 6G 資安解決方案。於廠商座談會中，將與國內資服資安業者、網通廠商與應用服務公司，以 Pre-6G 技術為出發點，綜合討論包含國際技術、市場趨勢、全覆蓋通訊專網商機及類型，著重探討國內軟硬體廠商及供應鏈的缺口及商機，相關產研專家之回饋與後續建議，為未來推動 6G 資安相關議題的重要參考依據，並據以研提對應推動機制，帶動國內技術研發與資安服務發展。

一、「支援零信任(ZT)架構的定期評估」座談會

(一)時間：112 年 5 月 17 日下午 14:00-16:00

(二)地點：台灣雲端產業發展協會大會議室(臺北市中正區重慶南路二段 51 號 8 樓)

(三)議程

時間	內容	主講者
13:30-14:00	報到	
14:00-14:05	開場致詞	資策會資安所 所長 何玲玲
14:05-14:25	分享1： 5G開放架構解決方案實例與產業發展趨勢	英業達(股)公司 處長 簡嘉南
14:25-14:45	分享2： Pre-6G網路的安全議題：以Open RAN 與非地面通訊的應用為例	資策會資安所 博士 蔡宜學
14:45-15:50	綜合討論：5G產業供應鏈廠商與談 1) 5G環境資安部署現況 2)從5G ORAN談專網零信任設計原則	主持人： 資策會資安所 技術總監 張文村
15:50-16:00	會議總結	

(四)會議參與廠商

共 14 家廠商參與，包含趨勢科技、訊勢科技、中華系統整合、中華資安國際、台達電子、伸波通訊、亞旭電腦、和碩聯合科技、英業達、凌群電腦、華電聯網、億宣應用科技、數聯資安與工研院產科國際所；另有本計畫協辦單位工研院、資策會長官擔任會議主

持以及執行單位台灣雲端物聯網產業協會長官共同與會討論，參與人數總共 25 人，其中包含 3 位女性(佔 12%)及 22 位男性(佔 88%)。

(五)會議結論

1. 建議通訊系統 ZT 架構可以建立一個產業界情資蒐集及通報體系，包含若有資安事件發生，可找到適合供應商即時處理的溝通聯絡支援管道。
2. 5G 網路層的問題複雜，建議政府優先推動 5G 應用服務商轉，同時公告通訊資安指引(Guideline)，指引針對產業特性會有不同面向從大架構到細項的定義，並在推動上消弭認知的差異或化解技術的歧異，市場機制會開始保護自己 5G 系統的資安作法。
3. 政府相關主管單位可以規劃 5G 垂直應用領域的機敏等級，去區分場域安全防護納管程度、在網路層必須重視什麼資安功能..等，建議客觀評級評測機制，較容易在大小不同的場域落實資安工作。

(六)效益說明

1. 分析現場與會廠商及與會者領域別包含研究單位、系統整合商、需求產業、資安廠商 4 類。在產業、工作領域上多與 5G / 6G 技術與應用、AI 技術與應用、資安議題有所關連，職務上則包含研究資安、管理企業資安或是自身已是資安廠商一員，對於會議設定欲從討論中收集產業意見目的具有良好的助力。
2. 與會者從不同面向領域出發，於會議中充分表達各自立場的想法與建議，強化交流網絡，促進資安廠商與產研之間合作交流有效促成原本立場對立的雙方換位思考尋求可能的共識。

二、「用 AI 感知世界 以資安防護未來」座談會

(一)時間：112 年 8 月 29 日下午 14:00-16:00

(二)地點：台灣雲端產業發展協會大會議室(臺北市中正區重慶南路二段 51 號 8 樓)

(三)議程

時間	內容	主講者
13:30-14:00	報到	
14:00-14:05	開場致詞	台灣雲協 物聯網資安SIG 副總召集人 何玲玲 (資策會 資安所所長)
14:05-14:10	貴賓致詞	數位部長官代表
14:10-14:40	分享1： 元宇宙中AIGC與虛擬人的應用	光禾感知 執行長 王友光
14:40-15:10	分享2： AIoT浪潮下資安產業發展趨勢	資策會產業情報研究所 MIC 資深產業分析師兼產品經理 童啟晟
15:20-16:20	綜合討論： 1) 5G、6G智慧系統AI模型不會被拷貝盜用 2)如何確保通訊層智慧系統元件能溯源管控	主持人： 工研院 資通所 技術經理 王邦傑
16:20-16:30	會議總結	台灣雲協 物聯網資安SIG 副總召集人 何玲玲 (資策會 資安所所長)

(四)會議參與廠商

共 12 家廠商參與，包含資策會產業情報研究所、光和感知、趨勢科技、訊勢科技、中華電信、中華電信研究院、全景軟體、拓樸科技、凌群電腦、華電聯網、未來映像、永豐餘生技。另有本計畫協辦單位工研院、資策會長官擔任會議主持以及執行單位台灣雲端物聯網產業協會長官共同與會討論。現場總共 21 人，其中包含 3 位女性(佔 14%)及 18 位男性(佔 86%)。

(五)會議結論

1. 偽 AI 需要從源頭開始重視：目前已有學研團隊發展 AI 模組可以做開源軟體(Open Source)，但內含一個隱型的 code 可以把輸出的生成圖像，判別是否為假圖像，是 AI 溯源的

作法之一，如何把學術性研究透過規範走到市場化，是一個思考的方向。

2. 5G、6G 專網的 Security 是 IoT 應用一環：通訊資安在 3GPP 已有基礎規範，但 AI 安全雖然有在倡議，還沒有明確規範，就會形成破口，怎麼讓 AI/ML 的駭客模組可以納入黑名單內追蹤，可以更好的防護到通訊網域安全，是技術上可以繼續努力的目標。
3. 數位產業只要有一個破口，整個產業的信譽就會大打折扣，所以需要政府政策的引導：包括人工智慧生成內容 (Artificial Intelligence Generated Content, AIGC) 有一個產業標準規範、AI 評測機制、車載資安需要發展全面性(含晶片、通訊網、聯網設備)安全防護方案。
4. 新興應用的資安框架：ZT 框架的安全，行動網路/系統網路的邊際失效是個趨勢，如何把 ZT 框架放在 5G、6G 的環境中，推動共通訊任機制，有一個一致性標準，可以有完整的解決方案。

(六)效益說明

1. AI 資安議題從應用到實務需求思考的串聯：透過元宇宙最新應用的國內廠商代表及國內領頭羊研究單位 MIC 分享近期最夯的 AIGC 應用與 AIoT 相關領域面臨資安議題，引導與會者多方面思考應用與防護彼此之間可能的問題。
2. 聆聽不同產業聲音，有效收集意見：對談廠商包括 Operator、專網維運商、系統整合、資安和研究單位等透過會議不同領域產業間，針對 AI 的資安議題進行討論與意見交流，有效達到本計畫欲收集不同面向意見收集的目的。
3. 資安廠商與產研共同發聲，理想與實務的搭配：與會者同意在 5G/6G/AI 都應於應用情境下展開相對應的資安布局，

跨領域跨平臺要有共同標準更是不可求，不同產業應有不同的資安標準，才能符合產業實際營運狀況，也才能漸進式的有效提升產業資安防護的能量。

三、「從 5G 到 6G 邊緣運算資安的變革與商機」座談會

第 3 場座談會於 112 年 9 月 19 日舉辦，座談主題為「從 5G 到 6G 邊緣運算資安的變革與商機」，會議中邀請包括資通訊應用服務、設備製造等跨域軟硬體業者。從數位發展部於 6 月初開放企業機構申請，智慧製造為主要應用場域，其次是智慧展演，預期專網帶動 MEC 應用商機，隨著網路通訊、演算法及邊緣運算的進步，企業逐漸開始將運算密集型應用程式的工作負載從資料中心移轉到邊緣端的應用出發，探討 6G 系統將會是第一個全面導入 AI 技術的自動化系統，邊緣運算是重要節點，需提升其高安全性與高可靠度等議題，建立適當的 MEC 資安保護機制。

(一)時間：112 年 9 月 19 日下午 14:00-16:00

(二)地點：台灣雲端產業發展協會大會議室(臺北市中正區重慶南路二段 51 號 8 樓)

(三)議程

時間	內容	主講者
13:30-14:00	報到	
14:00-14:05	開場致詞	台灣雲協 物聯網資安SIG 副總召集人 何玲玲 (資策會 資安所所長)
14:05-14:30	分享1： 由供應鏈安全看通訊產業鏈資安發展趨勢	工研院產科國際所 通訊與智慧聯網系統研究部 徐富桂 經理
14:30-14:55	分享2： 從5G專網加速數位轉型探討資安挑戰	CTOne 訊勢科技 易名揚 經理
14:55-15:50	6G系統將會是第一個全面導入AI技術的自動化系統，邊緣運算是重要節點，需提升其高安全性與高可靠度。在MEC端探討的資安問題包括： (1)邊緣運算虛擬化層(VM)的安全問題 (2)針對邊緣層機器學習模型和應用服務之威脅攻擊樣態分析資安解決方案	主持人： 物聯網資安SIG 博士 卓傳育 博士 (工研院 資通所組長)
15:50-16:00	會議總結	台灣雲協 物聯網資安SIG 副總召集人 何玲玲 (資策會 資安所所長)

(四)會議參與廠商

共 13 家廠商，包含工研院產科國際所、訊勢科技、中華系統整合、中華電信研究院、全景軟體、和碩聯合科技、凌群電腦、神雲科技、雲達科技、新電子科技、聯恩電子、邊信聯科技、趨勢科技。另有本計畫協辦單位工研院、資策會長官擔任會議主持共同與會討論。現場總共 21 人，其中包含 4 位女性(佔 19%)及 17 位男性(佔 81%)。

(五)會議結論

1. 國內業者的研發和驗測成本相較國際稍微偏高，政府單位若能於前期協助降低障礙會有極大幫助，建議國內資安規範能一致化，且依循國際資安標準制定，有助於業者後續接軌國際市場，也能減少 5G 專網場域主申請不同部會科專計畫時的產品設備資安驗證成本。
2. 若有資安檢測統一標準，可讓政府機關採購者和研發人員有參考和評估基準，降低採購及開發過程中的資安風險，另外建議可採分級檢測機制，某產品進入 A 場域須符合一級標準，當在進入 B 場域則需要符合二級標準時，廠商只要補增測項目即可，降低同樣產品進入不同場域的反覆檢測成本。
3. 資安投資就像買保險，沒出事就沒感覺，然而資安事件發生的後續投入成本反而更高，只是一般企業主對於資安的重視性，因看不到且需先投入維運資金而輕忽，建議政府推動更多成功案例，由大廠經驗來吸引一般企業主投入資安維護。
4. 資安是必然趨勢且力道越來越強，在 5G 到 6G 發展中，前端設備安全也備受重視，從設備金鑰、身分認證到稽核機

制都開始被要求，入網前檢測法規、入網後的維運檢測都很重要，必須定期安檢以避免資安漏洞一直存在著。

(六)效益說明

1. 5G 專網加速轉型，提升供應鏈安全重要性：透過工研院產科國際所與 5G 專網資安廠商分享通訊產業鏈與 5G 專網的資安發展趨勢與挑戰議題，藉此提升供應鏈安全重要性。
2. 收集產研媒體等單位聲音做為後續推動方向考量：通訊產業鏈資安趨勢交流討論對談廠商包括研究單位、系統整合商、5G/O-RAN 廠商、資安廠商等，透過會議不同領域產業間針對邊緣運算、攻擊樣態等資安議題進行討論與意見交流，作為後續建言推動考量方向。
3. 達成產研單位接軌國際之共識與期望：國內廠商研發與驗測成本高，未來建議朝國內資安規範如能循國際資安標準方向發展。

四、「B5G 邁向 6G 發展，萬物聯網探索資安應用新契機」研討會

(一)時間：112 年 10 月 5 日下午 14:00-16:30

(二)地點：台大醫院國際會議中心 203 會議室(臺北市中正區徐州路 2 號)

(三) 議程

時間	內容	主講人
13:30-14:00	報到	
14:00-14:05	開場、貴賓介紹	司儀
14:05-14:20	貴賓致詞	- 台灣雲協 物聯網資安SIG 總召集人 洪偉淦 (趨勢科技台灣區總經理) - 台灣雲協 物聯網資安SIG 副總召集人 何玲玲 (資策會 資安所 所長)
14:20-14:30	貴賓與講師群合影及全場大合影	
14:30-15:00	Keynote1： 通訊資安新興政策與技術趨勢面面觀 (TBD)	中央研究院資訊創新研究中心 主任 黃彥男
15:00-15:30	Keynote2： 後量子密碼(PQC)前瞻技術應用於6G網路安全研析	國立成功大學 教授 李南逸
15:30-15:50	Networking Time	
15:50-16:10	邁向6G O-RAN資安技術發展介紹	耀睿科技 協理 蔡志明
16:10-16:30	5G架構零信任，你所應該知道的一切	CTOne 訊勢科技 經理 易名揚
16:30~	會後交流、賦歸	

(四) 會議參與廠商

活動當天因小犬颱風因素，中南部部分縣市放颱風假，雖臺北無明顯風雨，亦因為報名者為外縣市人員，活動前來電表示無法參與，多少影響現場活動出席率，本場活動最終現場共 55 家單位廠商，共計 83 人共同參與，與線上報名人數 119 人相比，出席率近 7 成，與會來賓包含產學研單位，例如協會、研究單位、大專院校、醫療單位、國營事業、電信、系統整合商、電信設備製造/代理商、資安業、媒體者等。

(五) 會議摘記

1. 本場活動由台灣雲端物聯網產業協會物聯網資安 SIG 總召集人洪偉淦(趨勢科技臺灣區總經理)以及副總召集人何玲玲

(資策會資安所所長)聯袂出席，由洪總召集人開場致詞，為活動開啟序幕。

2. 中央研究院黃彥男主任提到 AI、IoT 是必須的發展，且因為 6G 會把應用帶向更好用與更快的方向，但如資安問題沒有解決，後續造成的災難以及如何控制災難會很難預測，但也是研究的方向。未來是否在以代理人的概念讓數位分身來進行工作、在網路詢問問題，不洩漏本人資訊，或許是可以思考的方向。
3. 國立成功大學李南逸教授則分享在當前 5G 的標準會延伸到未來 6G 的標準，資安問題亦同。5G 量子電腦的攻擊是最可怕的，所有協定、認證、加密、金鑰都會被破壞，所有的保護都會無效。以此為基礎討論未來以後量子密碼 (Post-Quantum Cryptography, PQC) 方式如何在 6G 環境中能有安全防護。新型的後量子認證與金鑰協議 (Authentication and Key Agreement, AKA) 的協定可望解決量子電腦威脅與攻擊，在金鑰封裝過程中以後量子密碼方式取代。傳統中會有 RANDOM NUMBER 可追蹤用戶，會遭遇鏈結攻擊。而在 PQC，則將 RANDOM NUMBER 轉換不用明文方式傳遞，讓攻擊無法辨識追蹤。駭客跟密碼學家的攻防是永遠不會停止的，因此後續還有許多研究方向。如何開始布局與使用 PQC 的演算法是關鍵，臺灣不能置身事外。
4. 耀睿科技蔡志明協理提到，在標準發展中，應發展 DU 與 O-RU 之間的授權應該走哪種方式是用何種具唯一性的憑證管理，這些都是現在 O-RAN 解離之後的標準中被探討的事情，這其中有些關鍵技術會與過去不同。5G 探討的資安議題中，國內已在陸續訂定有關 O-RAN 資安測試標準。

O-RAN 架構在政府的支持下已陸續在私網中布建。O-RAN 和現有 5G 基地臺最大的差異在具有智能控制及堆疊軟體的功能，在非近即時更具決策空間，AI 與 ML 也會進入到 O-RAN 控制端點以運用龐大資料庫，因此資安議題也值得被關注。

5. 訊勢科技易名揚協理則分享應如何保護企業 5G 專網，臺灣專網法對 5G 專網的規範以及廠商可以如何符合規範，在臺灣可以合法合規的布局、電信專用寬頻設置與管理辦法。企業導入 5G 專網後可大幅降低換線的複雜性程度甚至是縮短停線的時間，可反映到企業獲利。企業 5G 專網看起來是私網域，但實務上並非完全封閉，服務雲端化、軟體開源化、IoT 設備、邊緣設備可能就是被駭客入侵的破口，這其中邊緣運算端點是最容易遭受攻擊的。企業主與資安所所長針對 5G 專網的資安要求，應包含安全可視性、風險管控、一目了然的危機警示、防止偽基地臺、防堵開放原始碼等。

(六)效益說明

1. 有效達到新興資安概念推廣與擴散效益：議程設計以 B5G 到 6G IoT 產業應用的資安議題為主軸，颱風天亦吸引超過 80 位參與者到場參與，除了產學研代表，與會來賓包括電信業、系統整合商、電信設備製造/代理商、資安業者、中小型傳產企業、學生…等，逐步掌握潛在產品或業務推展契機。
2. 從資安危機到資安技術，有效提升資安意識：活動內容提供第一手 6G O-RAN 資安相關資訊，參與者持肯定態度且能藉由交流時間釐清問題，對資安議題的扎根與觀念推廣有很大助益，有助提升資安意識。

3. 提升 B5G/6G IoT 產業之資安能量：本場活動一方面藉由專家學者之公開演講來幫助與會者了解 B5G/6G 架構之資安威脅，並進一步剖析 5G ZT 架構的重要關鍵。另一方面，藉由活動之辦理及與會來賓之分享持續提升 B5G/6G IoT 產業之資安能量。
4. 現場設置技術展示攤位，提升資安議題交流度：活動現場設置資安技術攤位展示，參與者於報到後及中場休息時間有足夠時間與空間進行意見與技術需求討論，提升資安議題交流度。
5. 向下並下深度扎根，影響範圍觸及教育界與媒體界：本次參與者廠商單位相較於以往協會舉辦之資安活動，中大專院校以及媒體參與有明顯增加，顯見資安議題在學校相關科系中已經逐漸受到重視，而媒體對於本場活動內容亦有專篇報導，顯見資安議題除了產業重視之外，逐漸受到教育、媒體界的注意，更擴大本場活動之影響力。
6. 活動主題吸睛，參與者反饋期待後續活動：議程設計之主要議題(Keynote)講者從 6G 與 PQC 新興資安議題開場，帶出未來在企業或個人所面臨之各種資安議題須被重視的比重只會日益增加，後段由資安新創廠商輕鬆生動的說明 B5G 到 6G 資安產業技術與觀念建立，有效吸引參與者注意。
7. 講師分享內容吸引媒體目光，登上 DIGITIMES 報導：本場活動主題與講師分享內容吸引媒體注意，特別於活動後(10/6 及 10/11)刊登文章於官網，提升活動與資安重要性之曝光與推廣擴散度。

第五節 小結

在面對國際發展 5G 商用且同時布局新世代 6G 通訊技術發展情況下，我國應在此時此刻超前部署，及早盤點並掌握現階段國際主要國家、大廠所提出之 6G 先期研究主軸，同時思考現階段臺灣學研與產業技術研發能量的優勢和挑戰，投入 6G 技術發展的先期研究，規劃未來 6G 資安服務框架、推動業者參與探討未來場域中可能營運之狀況與對應推動機制，並執行 6G 資安產業研析與防護實證先導評估，與耀睿科技 OTIC 實驗室合作，針對核網特定元件如：AMF，發展資安攻擊樣態，測試攻擊發生的影響程度，建議導入之防護措施，同時對應與 ISO 27001：2022 標準之控制措施，驗證緩解方案可行性，做為發展 6G 網路軟硬體資安技術參照。

一、建議 B5G 邁向 6G 資安發展，政府政策引導並與國際接軌

本計畫針對目前正在發展的 5G 專網需求及邁向 6G 挑戰，與拜訪台灣電信產業發展協會、電信系統整合商及網通業者進行技術的交流討論，對應未來 6G 資安服務框架，多數業者表示隨著 5G 專網建置逐步推升，導致資安威脅增加的風險也備受關切，建議政府機構發布 5G、6G 通訊資安技術指引，逐步建構通訊網路安全管理制度；對應 6G 或 Pre-6G 加入 AI、BC 等新興技術之網路架構發展趨勢，亦建議要有常態性通訊資安技術交流討論組織，增加產業企業互動與合作機會，可凝聚產業聚焦優勢技術之發展共識，形成國內外技術同步的正向循環。

二、技術實證有利國內通訊產業擴增國際標準參與，取得商業先機

本計畫模擬 6G 跨領域應用環境，針對核網特定元件如 AMF 通訊標準身分驗證機制，提出「非有效終端設備企圖入侵正常基地臺與核網」、以及「偽基地臺與核網企圖影響正常終端應用服務」2 大類型 4 種資安攻擊情境，測試攻擊發生的影響程度，挖掘現行於 3GPP 國際標準規格遺留在行動網路中的安全問題，推導出防護緩解作法，對

應 ISO 27001:2022 控制措施「A.5.30 營運持續之 ICT 備妥性」、「A.8.9 組態管理」、「A.8.16 監視活動」建議導入防護作法，驗證緩解方案可行性，做為發展 6G 網路軟硬體資安技術參考，惟這類屬於遺留在原國際標準規格中須與時俱進的安全議題，最終仍建議回歸國際標準技術會議討論，方能從根本上解決。

三、舉辦產業 6G 技術交流活動，驅動廠商共識聚焦重點技術深耕

最後在參酌國際發展通訊資安趨勢及本計畫研究技術主題，於執行期間內分別於 5/17、8/29、9/19 及 10/5 完成 4 場技術交流座談會，會議中邀請包括專網維運商、系統整合、設備供應商、資安和研究機構等超過 50 家廠商(含因防疫線上參加)，取得不同參與者如何看待通訊世代的安全主題的面向，創新 5G 到 Pre 6G 資安解決方案，帶動國內技術研發與資安服務發展。

四、6G 資安發展趨勢與後續研發建議

研析 6G 資安發展趨勢，及相關潛力技術延伸的資安風險，預期未來 6G 基礎建設運作環境特徵將涉及超高速、超覆蓋、超節能、超低延遲、超信賴、超連結等，量子運算亦成為其中的關鍵技術之一，但高速運算的特性也引發新的資安議題，為了應對量子運算跳躍性的計算能力，目前全球也展開了次世代資安技術的研究與規格制定，其中基於密碼學為發展基礎的 PQC 為發展方向之一，PQC 新演算法可以保護資料免於量子電腦攻擊，並取代 RSA/ECC 等傳統密碼演算法，NIST 於 2016 年展開後量子密碼學標準技術挑選程序，選出可以抵抗量子電腦威脅（Quantum-Resistant）的密碼學系統，目標是選擇一套抗量子的公鑰密碼算法進行標準化，經過 7 年的努力，最終撰定 CRYSTALS Kyber、CRYSTALS Dilithium、FALCON 及 SPHINCS+等

4 種演算法成為第一批新一代安全標準^{5.12}，預計 2024 年標準將正式發布。

NIST 為美國制訂的標準，但其影響也將形成全球的標準，在現行 5G 認證安全機制中，識別用戶身分的 SUPI 會經過加密保護後，以單向的用戶隱藏識別碼(SUCI)進行身分認證，避免 IMSI 被竊聽，造成身分冒用或隱私洩漏等風險，然而在 5G 系統中，相互身分驗證和端對端加密仍然是未解決的問題，缺乏這 2 個屬性仍會導致誤操作、竊聽和追蹤攻擊，故 6G 架構中基於雲端和開放網路技術的動機，需要新的身分驗證，以便 6G 可以使用 5G 的安全概念，例如用於開放接取網路單一身分驗證平臺，將 PQC 適當整合到 6G 網路的硬體/軟體效能和服務需求中，強化加密和相互身分驗證，但需要評估可能會損害對延遲敏感的服務，雖仍處於量子運算的早期階段，採取措施為向後量子世界中安全密碼學的轉變做好準備。

5.12 CISA. (2022). Retrieved from <https://www.cisa.gov/news-events/alerts/2022/07/05/prepare-new-cryptographic-standard-protect-against-future-quantum-based-threats>

第六章 維運公部門連結小組

公部門連結小組由國家科學及技術委員會科技辦公室指導，針對 6G 發展各種議題，進行跨部會協商與意見整合。公部門連結小組整合包含雛型系統與國際布局、國際連結暨產業應用、頻譜整備及跨領域發展及部會合作與協調推進，共 4 個工作組如圖 136。本工作項目「公部門連結小組維運」屬部會合作與協調推進工作組項下，由本計畫辦理公部門連結小組會議、協助國際標準組織參與及建立國際合作管道/案例、觀測國際應用服務展及國內產業能量盤點共 3 項工作。

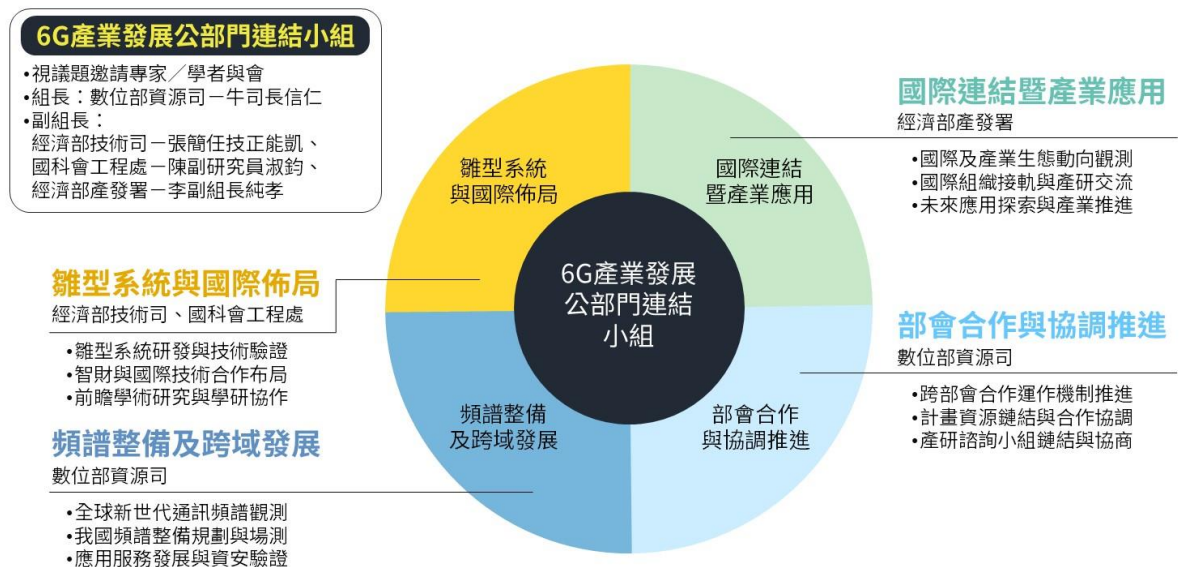


圖 136、公部門連結小組架構與分工

資料來源：本計畫整理

第一節 辦理公部門連結小組會議

公部門連結小組設立為聯繫「6G 產業發展先期研發計畫」，在本計畫推動下，每季至少辦理 1 場公部門連結小組會議，並規劃於產研諮詢小組會議之後召開，以掌握產業議題並進行公私部門資訊共享及協調作業，112 年度公部門連結小組會議時程如圖 137 所示。

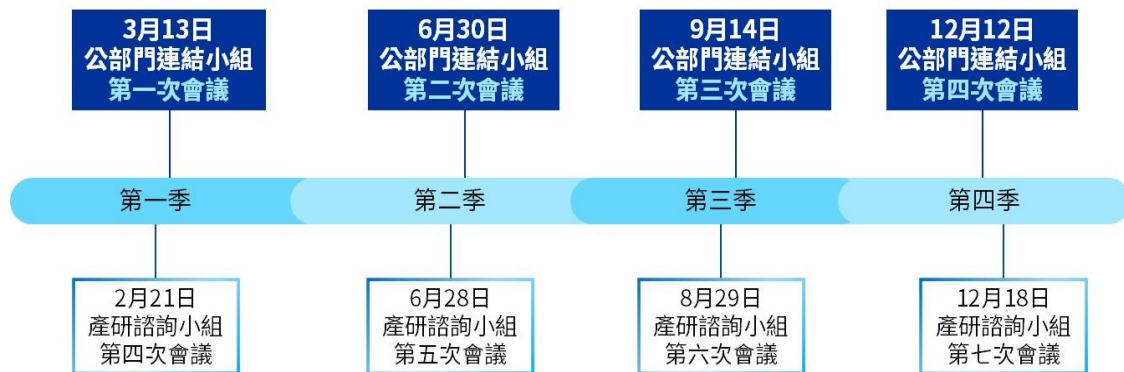


圖 137、112 年度公部門連結小組會議時程規劃

資料來源：本計畫整理

112 年度已辦理共 4 次公部門連結小組會議，分別包含規劃資訊協作平臺、研擬舉辦聯合大型研討會之可行性、公部門連結小組電子報之推動情形、3GPP 來臺之國際趨勢分享及資訊共享交流建議等，並於 112 年第 4 次公部門連結小組會議中說明 113 年相關規劃，歷次會議辦理情形說明如下：

一、公部門連結小組第 1 次會議

112 年 3 月 13 日舉辦，本次會議主要議題包含 3GPP 來臺舉辦第 100 屆會員大會、第一屆點子松得獎成果、巴塞隆納世界通訊大會 (Mobile World Congress, MWC) 會後趨勢研討會。除針對前一年度列管事項進行報告，並說明本年度公部門連結小組 4 場會議之規劃期程。另試行 2 期之《公部門連結小組電子報——6G 標準應用及觀測》

確定持續發布，後續由各工作組每月協助填報內容，由數位部資源司發報該電子報。

(一)會議議程

1. 報告事項

(1)歷次會議列管事項執行情形說明。

(2)本年度小組會議規劃及現況報告。

2. 討論事項

(1)MWC 會後心得分享交流規劃。

(2)112 年 6 月份 3GPP 來臺之國際交流事宜。

3. 臨時動議

「頻譜整備暨跨域發展」工作組提出「頻段需求現況調查」議題。

(二)會議結論

1. 考量點子松計畫中通訊及情境類之創意思維可作為各工作組 6G 應用參考，且得獎團隊可藉由各工作組將點子進一步落實於技術層面，請數位部於會後提供執行單位聯絡資訊予各工作組進一步交流合作。

2. 112 年 3 月 17 日舉辦「MWC2023 行動通訊大展重點趨勢研討會」，請於會後洽工研院產科國際所是否有相關可公開資訊得揭露於公部門連結小組電子報。

3. 國際組織 3GPP 來臺會議由聯發科技及台灣資通產業標準協會爭取主辦，請工業局追蹤並分享 3GPP 來臺活動資訊於電子報，相關可對外公開之成果請於交流後帶回公部門連結小組會議討論。

4. 維持現有電子報發行方式，發刊內容為未來 2 個月之相關國內外活動，包括純 6G 議題、資通訊相關領域議題等可完全公開供各界使用之共享內容。

5. 「頻段需求現況調查表」已放置於數位部資源協作平臺，各工作組亦可視需求提出協作議題，以利小組間資訊得以共享交流；另，「頻段需求現況調查」屬公部門連結小組內部之資訊協作平臺，不對外公開，僅供內部意見交換與討論之用。

(三)決議事項追蹤管理

會議議題	追蹤辦理情形
MWC2023 行動通訊大展重點趨勢研討會會後心得分享	經洽工研院產科國際所後，因活動簡報為非公開項目，故後續未揭露於電子報上。
分享國際組織 3GPP 來臺活動資訊於電子報	3GPP 來臺辦理會員大會相關活動資訊，已於 112 年公部門連結小組電子報 6 月版公布。
「頻譜整備暨跨域發展」工作組提出「頻段需求現況調查」議題	已有 1 案填報，與後續作業流程討論，列入公部門連結小組第 2 次會議討論案中進行討論。

二、公部門連結小組第 2 次會議

112 年 6 月 30 日舉辦，本次會議主要議題延續前次會議，包含 3GPP 來臺辦理會員大會後續成果、第二屆點子松活動以及是否有新的協作議題。並討論有關經濟部工業局辦理支持業者參與國際 6G 組織或活動，若後續有任何議題在提供資訊給各工作組參考。另外就頻譜資訊協作平臺作業流程進行調整，使其格式更臻完善。並就未來各工作組業管計畫原各自辦理座談或推廣活動，研擬聯合召開可行性。

(一)會議議程

1. 報告事項

- (1)歷次會議列管事項執行情形說明。
- (2)第一屆點子松得獎作品成果報告。
- (3)3GPP 第 100 屆會員大會後續報告。
- (4)公部門電子報發報概況。

2. 討論事項

(1) 第二屆點子松徵件及公部門連結小組參與。

(2) 資訊協作平臺實作狀況。

3. 臨時動議

各工作組研討座談會串聯規劃。

(二) 會議結論

1. 本年度 6G 產業發展先期研發計畫「支持業者參與國際 6G 組織或活動」預期關鍵成果項目，請工業局協助於資格審查結束後，提供申請業者之產業類別資訊予各工作組參考；另，審查通過之業者未來如參與 GSOA 國際衛星組織，請協助將國際熱門頻段及用途等資訊提供各工作組參考。
2. 有關屆點子松辦理之媒合輔導交流及跨域工作坊，請數位部策略司提供專家參與之具體細節予各工作組，由各工作組協助將前述資訊提供予各相關領域專家，並詢問參與意願。
3. 針對資訊協作平臺實作狀況，調整填報流程並請各工作組於 10 工作日內完成建議回復，回復建議原則依所業管領域提供回復，並擴充表單欄位，增設注意事項、需求方及回復建議工作組織聯絡方式。
4. 有關研討座談會串聯規劃，已建置「各工作組研討座談會調查表」於數位部資源協作平臺，請各工作組先行填報 112 年下半年預計辦理之座談或推廣活動資訊。預計於 113 年度辦理 1 場次大型聯合研討會，請各工作組編列本計畫預算及研提工作項目預作準備。

(三)決議事項追蹤管理

會議議題	追蹤辦理情形
第二屆點子松徵件及公部門連結小組參與	數位部策略司請各工作組提供專家學者名單，已確認由國科會工程處 1 名及數位部資源司 2 名專家學者，參與 9 月 15 日之媒合會及 9 月 23、24 日之工作坊。
資訊協作平臺實作狀況	填報與回復機制已依第 1 次會議決議更新。
各工作組研討座談會串聯規劃	已建置「各工作組研討座談會調查表」於數位部資源協作平臺，填報概況將於第 3 次會議中進行報告。

三、公部門連結小組第 3 次會議

112 年 9 月 14 日舉辦，本次會議主要議題包含經濟部技術處參與歐盟 EuCNC 2023 通訊大會國際交流分享，延續前次會議議題討論舉辦大型聯合研討會之規劃草案，後續進行盤點各工作組相關活動規劃。另為促進公部門間之先期交流合作，新增盤點年度參與國際相關會議，做為工作組各分項計畫成果分享規劃。

(一)會議議程

1. 報告事項

- (1)歷次會議列管事項執行情形說明。
- (2)公部門連結小組電子報發報概況。
- (3)歐盟 EuCNC 2023 通訊大會國際交流分享。

2. 討論事項

- (1)113 年舉辦大型聯合研討會之規劃草案。
- (2)公部門連結小組各分項計畫成果分享規劃。

(二)會議結論

1. 為提升公部門連結小組電子報資訊分享之完整性，後續將研擬於電子報中建置該超連結資訊。

2. 有關 113 年舉辦大型聯合研討會，以第 3 季為主要會議規劃時段，並由數位部資源司協助進行工作籌備及盤點各工作組活動規劃內容，包含時間、地點及議題安排等項目。
3. 為利橫向連結各工作組計畫執行內容及成果，請各工作組配合進行 112 年及 113 年參與 6G 相關國際會展調查作業。另規劃每季由 2 個部會進行分享議題，內容不限於計畫執行情形及國際發展趨勢，將適時納入未來本小組會議決議滾動調整。

(三)決議事項追蹤管理

會議議題	追蹤辦理情形
公部門連結小組電子報發報概況	電子報已建置連結，更新版本已於 10 月公布。
113 年舉辦大型聯合研討會之規劃	已建置「公部門連結小組舉辦國際研討會調查表」於數位部資源協作平臺。
公部門連結小組各分項計畫成果分享規劃	已建置「112 年及 113 年度國際會議參與調查表」於數位部資源協作平臺。

四、公部門連結小組第 4 次會議

112 年 12 月 12 日舉辦，本次會議主要議題包含第 2 屆點子松成果與得獎作品分享、112 年國際組織參與推動概況說明，以及 113 年公部門連結小組會議之規劃方向，包含辦理研討會、專題及國際趨勢分享規劃。

(一)會議議程

1. 歷次會議列管事項執行情形說明。
2. 公部門連結小組電子報發報概況。
3. 第 2 屆點子松成果報告。
4. 112 年國際組織參與推動概況說明。
5. 113 年公部門連結小組會議規劃。



(二)會議結論

1. 為促進小組間資訊共享，請各工作組踴躍填報資通訊相關領域之國內外活動資訊及議題於電子報。
2. 第 2 屆點子松得獎作品，供各工作組評估各作品技術落地應用之可行性，若工作組對於本屆得獎作品感興趣，歡迎隨時和點子松團隊聯繫。
3. 有關 113 年度公部門連結小組規劃之方向，經滾動調整後每季會議內容主要為專題分享，並視各工作組計畫成果、參與國際會議等進行提案分享。

(三)決議事項追蹤管理

因歷次公部門連結小組會議追蹤事項皆於本次會議解除列管，且本次會議無新增決議事項，故無需持續追蹤項目。報告事項及後續其他事項將於 FY113 延續計畫中持續辦理。

本計畫公部門連結小組會議詳細內容，請參閱附件 4 至 7。

第二節 協助國際標準組織參與及建立國際合作管道/案例

透過盤點國內外資源能量，整合國內產官學研，期促成共同參與國際組織或會議、建立國際合作管道或案例，本計畫現完成或協助之相關活動如下：

一、MWC 行前交流會

2023 年 MWC 於 2023 年 2 月 27 日至 3 月 2 日於西班牙巴塞隆納舉行，邀請各地手機廠商、軟體商、電信業者及無線通訊產業專家學者等參與，除展示新產品、服務和共同討論行動通訊產業相關之趨勢與技術，更提供企業、投資者及解決方案／技術提供商之間進行 B2B 媒合會議，為現今世界最具指標性的行動通訊相關會展。

本年度 MWC 會展如經濟部技術處、國科會工程處、國家通訊傳播委員會皆派員參加；同時由經濟部工業局籌組率 17 家廠商設置臺灣館。為整合國內公私部門能量，讓各與會單位串連相關資訊，共同參與國際盛會。由本計畫於 112 年 2 月 8 日辦理《MWC in Tawan-回顧 2022、展望 2023——MWC 行前交流會》。

本行前交流會邀集 MWC 參展部門及廠商，彙整前一屆重點議題、臺灣館展覽資訊；並介紹 MWC 2023 重點，如 5G/6G 網路基礎設施、AIoT 雲端服務、網路資訊安全、沉浸式體驗探索應用等議題。並由經濟部工業局介紹 MWC 2023 臺灣館的規劃重點、展出廠商類別及相關重要資訊。相關會議資訊如下：

(一)會議時間：112 年 2 月 8(三)上午 10 時至 12 時

(二)會議地點：集思交通部會議中心 202 會議室

(三)議程

1. 回顧 2022 MWC

2. 展望 2023 MWC：2023 會展主題、2023 臺灣館

3. 交流共享



二、MWC 會後資訊回饋

2023 MWC 會後，共有由工研院產科國際所舉辦《MWC 2023 行動通訊大展重點趨勢研討會》及資策會產業情報研究所舉辦《MWC 2023—預見通訊智能新未來研討會》。由本計畫協助轉發相關活動資訊於 112 年 3 月版公部門連結小組電子報中。並積極接洽工研院產科國際所，為公部門連結小組各工作組保留參加名額，共協助 4 名工作小組成員完成參與。

三、3GPP 第 100 屆會員大會及經濟部工業局辦理 112 年 6G 國際組織參與支持機制提案徵選

3GPP 於 112 年 6 月 12 日至 16 日於臺北南港展覽館舉辦第 100 屆會員大會。經濟部工業局亦舉辦相關周邊活動，包含工作坊、交流分享活動，掌握下世代通訊技術及標準發展動向，亦可及早盤點、布局我國切入點，並與國際大廠深化研發合作關係，強化未來 6G 通訊國際合作機會。

本工作小組於 112 年 6 月 30 日公部門連結小組第 2 次會議，邀請經濟部工業局報告相關活動辦理情形，以及說明所辦理之 112 年 6G 國際組織參與支持機制提案徵選計畫，並研商與其他工作組合作之可行性。

第三節 觀測國際應用服務展及國內產業能量盤點

一、資訊共享平臺

為促進公部門連結小組資料共享及交流，透過觀測國際應用服務發展趨勢，進行國內產業能量盤點，為此建立《公部門連結小組電子報——6G 標準應用及觀測》，共享國內外 6G 相關活動、會議及資訊。

(一)填報內容

由 6G 產業發展公部門連結小組各工作組填報可完全公開之資訊，共分類為：

1. 國內活動：蒐整國內相關領域之講座、會議、工作坊等資訊。
2. 國際活動：蒐整國際相關大型商展、國際會議資訊。
3. 共享資訊：包含國內外各組織、公司所發布之白皮書、產業報告相關領域重要報告。
4. 重要成果摘要：由 6G 產業發展公部門連結小組各工作組項下執行之計畫，並於報告完成後提供可供開之報告資料。又 6G 行動通訊發展與 5G/B5G 有密切關聯，內容不侷限於純 6G，相關聯產業發展皆可提供。

(二)填報方式

由數位部資源司設置電子報提供共筆格式，各工作組於每月 15 日前填報電子公開資訊，並由數位部資源司負責彙整及簽辦發報作業，其中國內外活動揭露資訊以該期電子報未來 2 個月相關活動為主，如圖 138 所示。每月底至隔月初於完成電子報發報，並放置於數位部官網。



圖 138、電子報填報及發刊規則

資料來源：本計畫整理

自 112 年 2 月份發報第 1 期，至 112 年 11 月止，已發報共計 11 期電子報，相關電子報發報情形如表 50：

表 50、112 年度電子報填報概況

類別 \ 月份	2	3	4	5	6	7	8	9	10	11	12	總計
國內活動	2	2	2	4	2	1	1	3	3	3	1	24
國際活動	2	4	6	4	3	3	3	3	2	3	1	34
資料分享	4	2	4	5	7	6	7	4	4	4	4	51
成果報告	0	0	1	1	0	2	0	0	0	0	2	6
總計	8	8	13	14	12	12	11	10	9	10	8	115

資料來源：本計畫整理

本計畫公部門連結小組電子報詳細內容，請參閱附件 3。

二、規劃資訊協作平臺

針對 6G 發展各項議題，為達成各工作組間之統合協作議題、提供各產學研界研擬方向之可行性、意見交換等目標，於公部門連結小組內部資訊系統建置「資源協作平臺」，本平臺屬公部門連結小組內部意見交換與討論之用，不對外公開，並非代表機關最終決定。

112 年度為因應「頻譜整備暨跨域發展」工作組提出「頻段需求現況調查」議題及「各工作組研討座談會串聯規劃」，已建置「頻段

需求現況調查表」及「各工作組研討座談會調查表」，相關辦理情形說明如下：

(一) 頻段需求現況調查表

因應頻譜整備暨跨域發展工作組提出「頻段需求現況調查」議題，以及國內 6G 產業技術發展，建置頻段需求現況調查表，調查範圍為發射地點、電臺類型、涵蓋範圍、發射頻率、使用頻寬、最大發射功率、使用目的及相關意見回饋，調查結果將作為各工作組 6G 產業發展之技術參考。

調查表為每季統計填報狀況並於公部門連結小組會議報告，自 112 年 3 月 13 日經 112 年公部門連結小組第 1 次會議通過並執行開放該調查表填報，目前已有 1 筆資料填報。經 112 年 6 月 30 日公部門連結小組第 2 次會議討論該填報內容，並滾動式修正填報表格式，現調查表格式如表 51：

表 51、頻段需求現況調查表

注意 事項	1.國際電信聯合會(ITU)為利頻率支配(Allotment)，其中我國全境範圍皆劃歸於第 3 區域(Region 3)，為利確保未來所開發產品得以在市場順利流通，建議優先挑選符合中華民國無線電頻率分配表所載用途種類之對應頻段，並向相關主管機關申請進行測試。									
	2.我國中華民國無線電頻率分配表，詳見： https://s.moda.gov.tw/b55aKDnsdcyu									
	3.數位發展部無線電頻率使用管理辦法相關書表，詳見：									
	https://s.moda.gov.tw/TsCXs2yszTRX									
需求者	聯絡人、聯絡電話	發射地點	電臺類型	涵蓋範圍	發射頻率	使用頻寬	最大發射功率	使用目的或用途	建議回饋	業管聯絡人
(機關/單位)	(聯絡人、電話)	(詳細地點)	(固定臺/行動臺/固定+行動臺)	(詳細位置及範圍)						

資料來源：本計畫整理

(二)各工作組研討座談會調查表

針對產研諮詢小組提出之「各分項皆邀請專家群，技術面、標準面及頻譜面，如何相互交流整合？」議題，依 111 年 9 月 23 日公部門連結小組第 1 次會議決議，請各工作組研擬舉辦聯合大型研討會之可行性，以利專家學者於會議交流整合意見，及讓業界了解政府將持續積極協助。

經 112 年 6 月 30 日公部門連結小組第 2 次會議通過並執行「研討座談會調查表」，由各工作組先行填報 112 年下半年預計辦理之座談或推廣活動資訊，調查表格式如表 52：

表 52、各工作組研討座談會調查表

機關/單位		
計畫名稱	座談會項目	預計舉辦期程
	(座談或推廣活動主題)	(年月)

資料來源：本計畫整理

各工作組研討座談會調查表經統計後，112 年度較聯合舉辦之可行性，經 112 年 9 月 14 日公部門連結小組第 3 次會議決議，後續將以 113 年第 3 季為主要會議規劃時段，為籌劃活動各項作業，包含時間、場地及議題安排等相關活動細節，由各工作組配合填報活動規劃調查表，調查表格式如表 53：

表 53、113 年公部門連結小組舉辦國際研討會調查表

填報單位	座談活動 議題	建議邀請專家學者名單			
		姓名/職稱	任職單位	專長領域	聯絡方式

資料來源：本計畫整理

(三)盤點年度參與國際會展調查表

為利各工作組與相關合作團隊橫向整合各界能量，經 112 年 9 月 14 日公部門連結小組第 3 次會議決議，除循例於每年第 3 季盤點下一年度參與 6G 國際相關會展外，新增盤點當年度已參與國際會議，並做為工作小組之潛在報告候選議題。由各工作組配合填報 112 年及 113 年參與 6G 相關國際會展調查作業，調查表格式如表 54 及表 55。

表 54、112 年度國際會議參與後調查表

填報單位	會議名稱	參與議題	參加團隊名單	參與情形	備註
				(線上/ 實體)	

資料來源：本計畫整理

表 55、113 年度國際會議參與調查表

填報單位	會議日期	會議性質	會議名稱	參與議題	主辦方	預計參加團隊名單	預計參與情形	建議其他共同參與之利害關係人
	(月 / 日)	(學術論文 / 標準科技、經貿交流 / 國際組織等)					(線上/ 實體)	

資料來源：本計畫整理

第四節 小結

接續 111 年度所建立之公部門連結小組，於 112 年度已辦理 4 場公部門連結小組會議、3 案國際合作，並製作共計 11 期公部門連結小組電子報與 3 個公部門連結小組資訊協作平臺。

一、辦理公部門連結小組會議

112 年度已辦理共 4 次公部門連結小組會議，對 6G 發展各項議題進行跨部會協商與意見整合，分別規劃資訊協作平臺、研擬舉辦聯合大型研討會之可行性、公部門連結小組電子報之推動情形、3GPP 來臺之國際趨勢分享及資訊共享交流建議。並因應議題需求邀請相關專家學者與會參與討論，以期有效進行計畫滾動修正。

二、協助國際標準組織參與及建立國際合作管道/案例

112 年度本計畫已建立共計 3 案國際合作管道，使我國可跨部會並串連公私部門能量參與如 MWC、3GPP TSGs 等大型國際盛事。後續會持續彙整國際組織資訊及國際活動參與資訊串聯各工作組任務，達成整合國內產官學研，期促成共同參與國際組織或會議、建立國際合作管道或案例。

三、觀測國際應用服務展及國內產業能量盤點

透過公部門電子報發行，有效蒐整國內外會展活動資訊，方便各工作組於活動參與前可橫向連結，共享資訊；另彙整國際上具指標之組織如 ETSI、NEXT G Alliance 等，及相關領域公司公開之白皮書、技術報告，使各工作組可及時掌握 6G 技術及其應用發展之最新狀況。

本計畫持續維運公部門連結小組，使公部門相關計畫間的資訊更為通透，整合國內能量，共同參與國際盛會，期帶動新型應用服務及系統整合發展。

四、未來公部門連結小組運作強化

公部門連結小組運作，依 6G 產業發展先期研發計畫規劃，針對 6G 發展各項議題進行跨部會協商與意見整合。除賡續 112 年度所規



劃之資訊共享平臺——公部門連結小組電子報，及每季至少召開 1 次公部門連結小組會議外，應持續針對各部會之需求，進行滾動式修正。建議邀集各部會分享分項計畫之執行概況，及會議參與回饋，以互相溝通各分項計畫執行內容，掌握發展目標與方向。此外共同加強多邊的交流，邀請產官學界專家及學者透過公部門連結小組進行分享交流國內外發展趨勢及技術運用等資訊，並且舉辦相關大型研討座談會，邀請海內外 6G 及資通訊領域優秀研究者，分享相關趨勢及展望。

第七章 研析與實證成果

第一節 跨領域應用

一、建立 6G 跨領域應用情境之參考架構先導評估

Cloud-Native 的機制提供網路管理層面另一種實現選擇方式，針對目前所謂的 SDN 利用 Cloud-Native 中容器化、微服務化特性，將會繼承在應用層的效益，對於網路管理機制也具備彈性化、效率、自動化同等效益。Cloud-Native 技術將對於未來 6G 無線網路環境產生積極的益處，擴充 6G 無線網路在擴充性、故障恢復、自動化、快速部署和更新等功能的強化，將效益自應用服務層面拓展至網路管理層面。

在普遍的認知中 AI-Native 是未來 6G 行動網路系統必要特徵之一，特別強調在整個系統的生命週期中全面應用 AI 技術，而不僅僅是一個附加功能。在規劃、設計、開發和部署時，即將 AI 技術融入到核心中，更緊密深入融合到 6G 系統架構、網路元件和作業流程之中，展現出更高的智慧、自主性和創新性的特性。

本計畫就能力、服務、架構技術 3 個面向解析 6G 行動通訊系統下實現 AI-Native 的需求條件，考量各面向中在運算資源、AI 演算法和資料 3 要素的需求，期帶未來 6G 網路能支援差異化、客製化的 AI 能力和服務應用，建構堅實的 AI 應用基礎，以支援未來更多以 AI 為基礎的新興商業模式及應用。

以智慧商店商品辨識新增類別應用比較 CNN 及 CIL 演算法效能。CNN 在新類別時辨識正確率較佳，但對舊類別表現較差；CIL 則可維持穩定正確率但需較長訓練時間。故應根據需求選擇適當演算法。

6G 的關鍵指標高容量和低延遲(每平方公里 1000 Gbps 的傳輸量及 1 毫秒以下的低延遲)使得大型機器學習模型(如 CNN、CIL)的傳輸和執行變得更加可行，這有助於未來 Edge 端整合的各種應用，包

括智慧商店、智慧工廠及智慧城市等。

二、規劃與建立安全與可靠的 6G 跨領域應用機制與技術先導評估

6G 之關鍵績效指標所宣示的高規格技術，致使無線網路營運商需分享電信基礎建設以降低成本，也需共享行動用戶資料以最佳化網路效能，無需事先有信任關係即可使用行動網路資源的新型態安全框架取代現行安全框架。經由文獻收集及分析，發現各國國際組織都想藉由 DLT 技術建構新型態的安全框架來達成資料共享：

(一)ETSI

ETSI 的白皮書介紹 DLT 及 PDLT 技術，並在標準說明如何建置/使用 BC，同時在建議核心網路須連上 BC，以及不同 BC 的互通說明。

(二)ISO

ISO 說明如何建置/使用 BC 標準為 ISO/TR 23455，雖然 ISO 有關 BC 標準的推動者為 ETSI，但此標準未明訂以 PDLT 為建置 BC。

(三)ITU

在 ITU_Y.2342 和 ITU_Y.3530 2 個標準說明如何建置與使用 BC，同時在說明不同 BC 如何互通。

除新型態的安全框架之需求，資料共享還需要分散式儲存系統，上面所提的標準都隱含使用 BC 為分散式儲存系統，以達成安全與可靠的需求，較明確指出如何建立分散式儲存系統有 ETSI 白皮書中的補充文件。若是考慮 IoT 應用，ITU-T. Series F 則是明確定義使用 BC 用於存放 IoT 應用資料的分散式儲存系統。

就目前收集的文獻分析研判，國際組織並沒有建議 BC 或是 IoT 系統部署於 MEC 運算架構，只有在 ITU 已提案的討論群組建議將 BC、IoT 及 MEC 結合 ITU_Y.4486。此趨勢亦 ETSI 白皮書定義 MEC 是具有儲存能力以及計算能力，並有虛擬化能力(使用 SDN、NFV 實



現動態配置網路元件)，而 IEEE 則以 BC、IoT 及 MEC 發展電子病歷應用系統。

使用 DLT 建置分散式認證機制及儲存系統，將資料及計算都留在邊緣運算環境的可行性，經過與中央式認證機制比較，基於 DLT 的認證流程，確實可以降低延遲，提升分散式系統建至於邊緣運算環境建的可行性。在結合 IPFS 與 BC 所組成的分散式儲存系統方面，由於 BC 提供不同參與者建立信任的機制與審計能力，使得結合 IPFS 與 BC 之分散式儲存系統適合用於發展跨不同公司或組織的資料分享平臺，同時保有邊緣運算環境低延遲、快速連結等優勢。

第二節 資安產業研析

一、建立 6G 應用自動攻防與情資雛型系統先導評估

在 6G 標準制定仍然在全球熱烈討論之際，對於 6G 應用安全性的研析，不僅至關重要，更可以確保未來通訊技術在國內廣泛部署時，能夠提供穩定、強健、可靠的防護機制，降低潛在資安風險，提升未來 6G 應用資料的安全性與隱私保護。從 AI-Native Security、in-X 子網 Network Slicing Security、IP Spoofing、DoS、Downgrade Attack⁵ 種資安威脅進行研析，從現有 5G 通訊環境切入，研析成果說明 5 種威脅潛在的攻擊模式，並針對防禦或緩解措施，提出可能作法。對於後續進入先導評估階段，指出一個明晰方向和策略框架。

資安防護測試永遠不嫌多，對於相關情資流通交換更是整體防護產生效果的重要關鍵。本計畫團隊針對滲透測試相關規範進行研析，NIST SP 800-115 第五章第二節滲透測試流程：規劃(Planning)、發現(Discovery)、攻擊(Attack)、報告(Reporting)，已成為所有滲透測試的標準流程，這個程序被廣泛採納，5G 核心網路測試、IoT 滲透測試，都在這個基礎上，建立各自的測試項目。而未來 6G 將可基於這些測試項目，發展出因應 6G KPI 所衍生的新測項目。共通情資交換格式是建立成功聯防體系的關鍵一步，國內 N-ISAC 以 STIX v.2.1 為基礎發展出國內的情資交換格式。針對 STIX 的研析發現國內的情資交換格式在資安事件的「攻擊 IP」與「受駭 IP」僅能呈現 IPv4，因而提出 2 種可能的解決方法做為參考。

鑒於未來通訊系統架構的功能切割，以及特定場域的應用(亦即專網應用)普及化，邊緣運算在未來 6G 運算環境中，將扮演重要的角色。本計畫在先導評估的情境設定即是以邊緣運算平臺為基礎，運用上述威脅研析成果以及規範研析成果，規劃先導評估的實測項目，應用容器連線行為監控技術，建立容器連線行為常模，僅容許常模連線封包通過，阻擋未經許可的連線行為。因此可以阻絕 DoS、IP Spoofing

等威脅攻擊，並透過共通情資交換格式快速通報偵測攻擊資訊，達到資安聯防共同阻斷威脅擴散的成效。

二、6G 資安產業研析與防護實證應用驗測先導評估

2019 年全球首屆 6G 峰會在芬蘭召開，各國頂尖通訊專家共同擬定全球首份 6G 白皮書，6G 網路正式成立為一個研究領域，自此之後，越來越多政府和組織宣布將邁入 6G 研究。6G 網路與 5G 不同之處，在於還沒有標準的功能或規範，只研究多種可能性應用，在此框架之下，6G 網路將不僅是 5G 網路的更快版本，而是 5G 技術各方面的提升，如覆蓋範圍不像 5G 網路那樣僅限於陸路，而是提供完整的陸海空域覆蓋網路。且 6G 網路應該具有更高的 AI 能力，事實上，在很多研究人員看來，6G 網路應該是「AI 賦能」的網路，AI 既是其驅動力，也是其最突出的特徵。

6G 網路包括「實時智慧邊緣運算」、「分佈式 AI」、「智慧無線基地臺」和「陸海空 3D 通訊網路」共 4 項關鍵技術，這些關鍵技術涵蓋迄今正在進行 6G 研究中最有力的部分。但仍受到最嚴重的安全和隱私問題影響，最主要的問題在智慧無線臺容易受到身分驗證、訪問控制和惡意行為的影響，尤其是實時智慧邊緣運算和智慧無線基地臺一起運作時，在抵禦惡意行為和數據傳輸過程方面特別薄弱。對應 6G 關鍵性技術指標，須優先提出系統可靠性、安全和隱私的安全技術議題與提出風險緩解措施建議方案。

「6G 資安產業研析與防護實證應用驗測先導評估」模擬 6G 跨領域應用環境，針對特定 Pre-6G 組件，如 AMF，發展 4 類型資安攻擊腳本有關帳號驗證、訪問控制、數據傳輸。目的在驗測 6G 環境下，由產研共同聚焦 Pre-6G 資安技術驗證，將測試結果透過國內 OTIC 實驗室回饋至國際 O-RAN Alliance，形成國內外前瞻技術探討與同步的正向循環。



第三節 維運公部門連結小組

為促進跨部會之間溝通及良好的訊息傳遞，112 年度已辦理共 4 次公部門連結小組會議，對 6G 發展各項議題進行跨部會協商與意見整合；與此同時也彙整 6G 相關資訊以公部門連結小組電子報發布，使各工作組訊息有效橫向連結。

後續會持續依前述形式，透過上述公部門連結小組會議報告相關資訊及國際性交流活動，整合國內外 6G 相關活動、會議資訊及因衍生之政策議題，於每月定期發報電子報，並因應公部門連結小組會議議題需求，規劃建置資源協作平臺，以達資源共享及意見交流，作為未來 6G 產業技術與發展方向之參考。

第八章 結論與建議

第一節 短期可行建議

5G 行動通訊系統為 ITU-R 依據全球國家決議於 2020 年所完成之標準系統，該無線電標準系統為一個能支援各種應用，具有彈性及多種發展可能性之網路系統，將帶動全球資通訊產業與網路系統之布建與產業發展之進程。對於 2030 年下階段全球 6G 行動通訊系統之實現，全球產業皆普遍認知將延續 5G 發展架構與概念，持續改造目前資通訊產業環境與商業模式。在 ITU-R 之後續規劃下，隨著 6G 應用更極致化的應用需求，6G 技術亦將根據各種不同應用場景，實現各種專屬之技術方案，以迎合 6G 時代之新服務需求。

而在聯合國 2030 年全球永續發展目標下，6G 標準系統已經正名為 IMT-2030，並被賦予從行動通訊角度實現特定目標之任務，從現有 5G 之架構與應用，延伸至 6G 亦可使用之相關應用架構與資安方案，可視為本計畫短期研究方向與發展目標，既可銜接既有 5G 應用，亦無需在邁入 6G 的轉換過程中被淘汰。

參考目前數位部以及相關政府政策方向，以安全與韌性的角度看待跨領域應用，可基於 6G 的 9 大應用趨勢(詳述於第二章第一小節)，對應相關智慧應用與領域情境，發展融合 ZT 架構與資料保護的技術，先於 5G 場域導入相關體系與架構，並逐步改善優化，持續延伸至未來的 6G 應用。

而以本計畫既有之成果，亦可建立相關主題之建議方案或案例作法，提交至與 6G 跨領域應用相關之公協會(如台灣資通訊產業標準協會、台灣雲端物聯網產業協會等)做為參考與推廣，例如：台灣資通訊產業標準協會的工作委員會「TC1：前瞻行動通訊」、「TC3-裝置聯網工作小組」、「TC-5 網路與資訊安全工作小組」，聚焦推動 B5G/6G 相關國際/區域標準連結，布局未來 B5G/6G 國際標準核心技術，即

可將本計畫對無線接取網路技術，測試實證現行國際標準仍可接取假基地臺與核網，以致終端設備的資料外洩的成果，透過國內產業探討評估解決方法，透過台灣資通訊產業標準協會提案標準修訂，同時協助產業在現有 5G 相關應用服務往未來 6G 邁進時，先期建立相關參考案例與概念，減少過程中可能遭遇的問題。

而從目前多數領域，包含 5G 邊緣雲的場域應用，都考慮生成式 AI 應用導入，結合本計畫對 Cloud-Native 的探討與規劃，可規劃目前已有的生成式 AI 技術於通訊相關場域，銜接未來 6G 9 大應用趨勢，如普適運算、沉浸式多感媒體整合與數位孿生虛擬世界等，建立前期的概念性驗證。

第二節 中長期建議

6G 將會需要更靈活且高度虛擬化的網路基礎設施，以支持不同的應用和服務。運用 Cloud-Native 概念可以應用於 NFV，將網路功能拆分成輕量級的虛擬化單元，並使用容器技術來部署和管理虛擬化功能。透過 AI-Native 的導入，此概念被業界認為是未來 6G 行動系統的核心架構特徵之一。基於電信基礎設施普及之現實優勢，將會更加彰顯出 AI 效能提升和價值，協助實現未來 6G 無線網路的願景實現。

以中長期方向來看，運用 Cloud-Native 與 AI-Native 結合 6G 9 大應用趨勢，可用作以 6G 獨有特色之應用情境與技術為規劃或嘗試方向。

如未來 6G 之 NTN 通訊，可實現允許用戶發送訊息、接收緊急警報和定位數據，填補地面蜂窩網路覆蓋的空白，並支援智慧手機實時語音和視訊通話，提供無縫的連網體驗。但 NTN 在實現高覆蓋的同時，犧牲了頻寬，因此相關特定應用，如人機協作救災、搜索或是透過智慧化無人載具進行緊急物資運送等，就需要高度的通訊整合與 AI 協作，可在頻寬高低不同與覆蓋面積不同之狀態下，啟動適應當

下情境的 AI 應用服務或是認證機制，輔以容錯機制與分散式架構等，建構符合 6G 智慧化與普適化目標的可靠服務機制，相關技術上之需求即包含適應各類型應用與通訊覆蓋情況下，須以任務目標為導向之 AI 應用調配與連結，模型融合與派送等，並且以目前歐盟與美國、ISO 之發展方向來看，未來不僅僅是高度應用 AI 組合相關服務以增進效率，亦需要配合對 AI 監管之需求，對 AI 進行測試與安全驗證，尤以 6G 為國家基礎建設之角度視之，更需要審慎評估其風險與回復方案。

另外為強化公部門小組運作，持續促進 6G 產業先期發展研發計畫各工作組橫向連結，建議透過全盤資訊收集，滾動掌握各項計畫所關注資訊之國內外應用發展政策及趨勢，並回饋具體可行資訊，作為公部門連結小組各工作組整合協調方向，可考慮透過邀集各部會分享參與國內外會議之狀況及成果計畫，以相互掌握發展目標，並應共同加強多邊交流，邀請產官學界專家及學者透過公部門連結小組會議，進行國內外發展趨勢及技術運用等資訊分享交流，並更有效地檢視規劃發展路徑，使各項計畫得以更有效溝通與推動。

第三節 計畫 4 年執行架構

本計畫參照現有 6G 產業發展先期研發計畫至 115 年之規劃，擬定至 116 年之執行架構。延續本計畫的跨領域應用規劃，有鑑於 AI、資安隱私與網路覆蓋為未來 6G 發展重要議題，研析具備資安與隱私防護機制的 AI、混合式網路與 6G 通訊特性整合跨領域應用，帶動國內產業超前部署 6G 應用技術。其中亦包含運用公部門連結工作小組，針對 6G 發展各項議題，進行跨部會協商與意見整合。

相關發展對應 2023 年 6 月 22 日在第 44 屆 ITU-R WP 5D 會議上定稿之 IMT-2030 (6G) 新建議書中，ITU-R 的主要目標是就 IMT-2030 (6G) 的全球願景達成共識，包括潛在的用戶應用趨勢和新興技

術趨勢，定義增強型和全新的使用場景以及相應的解決方案、能力，以及了解新的頻譜需求。

其中所描述的未來 6G 發展的時間線與應用場景，在 IMT-2030 期程上(如下圖 139)，將會對應新興技術趨勢包括 AI-Native 等技術——指的是支持 AI 的空中接口設計和用於 AI 服務的無線電網路、集成傳感和通訊、THz 傳輸、大規模多傳入/多傳出天線系統(Massive Multi-Input Multi-Output, Massive MIMO)和智慧表面技術(Reconfigurable Intelligent Surface, RIS)、通過分散式帳本和量子技術增強可信度，以及地面網路(Terrestrial Network, TN)和 NTN 之間的互連。

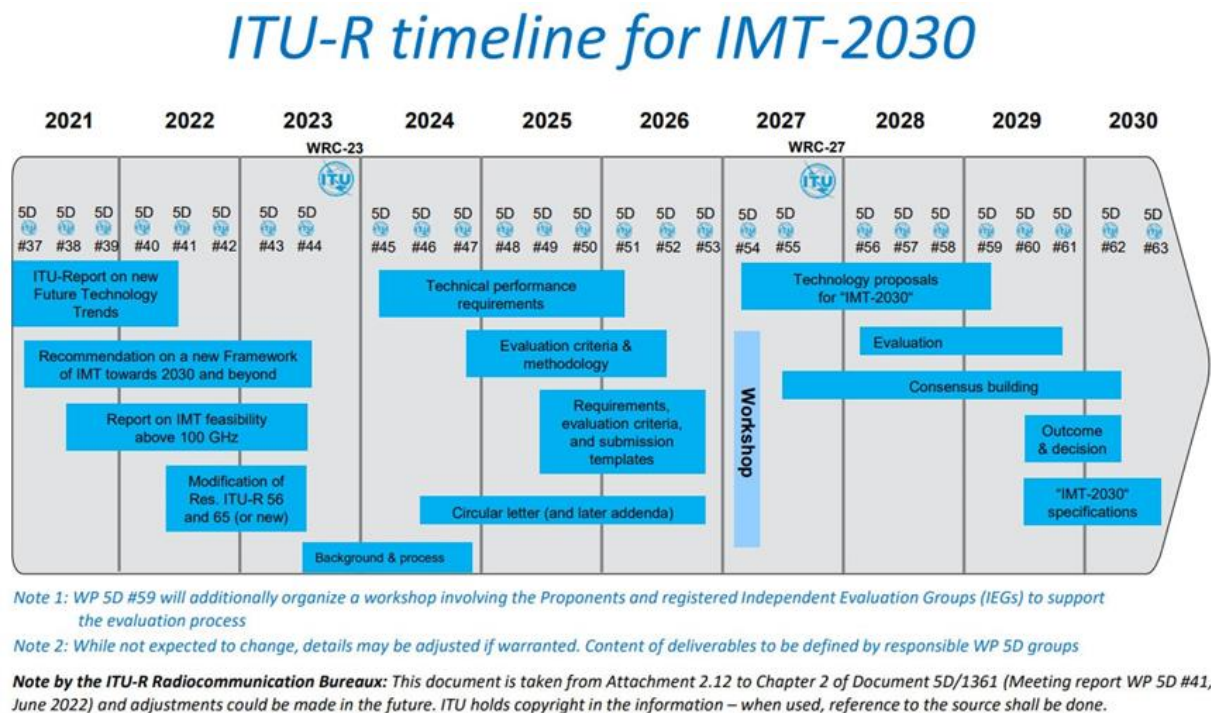


圖 139、2030 ITU-R IMT-2030 期程

資料來源：請參閱附錄-參考資料^{8.1}

8.1 ITU-R. (2023). Overview timeline for IMT towards the year 2030 and beyond. Retrieved from <https://www.itu.int/oth/R0A060000C8/en>

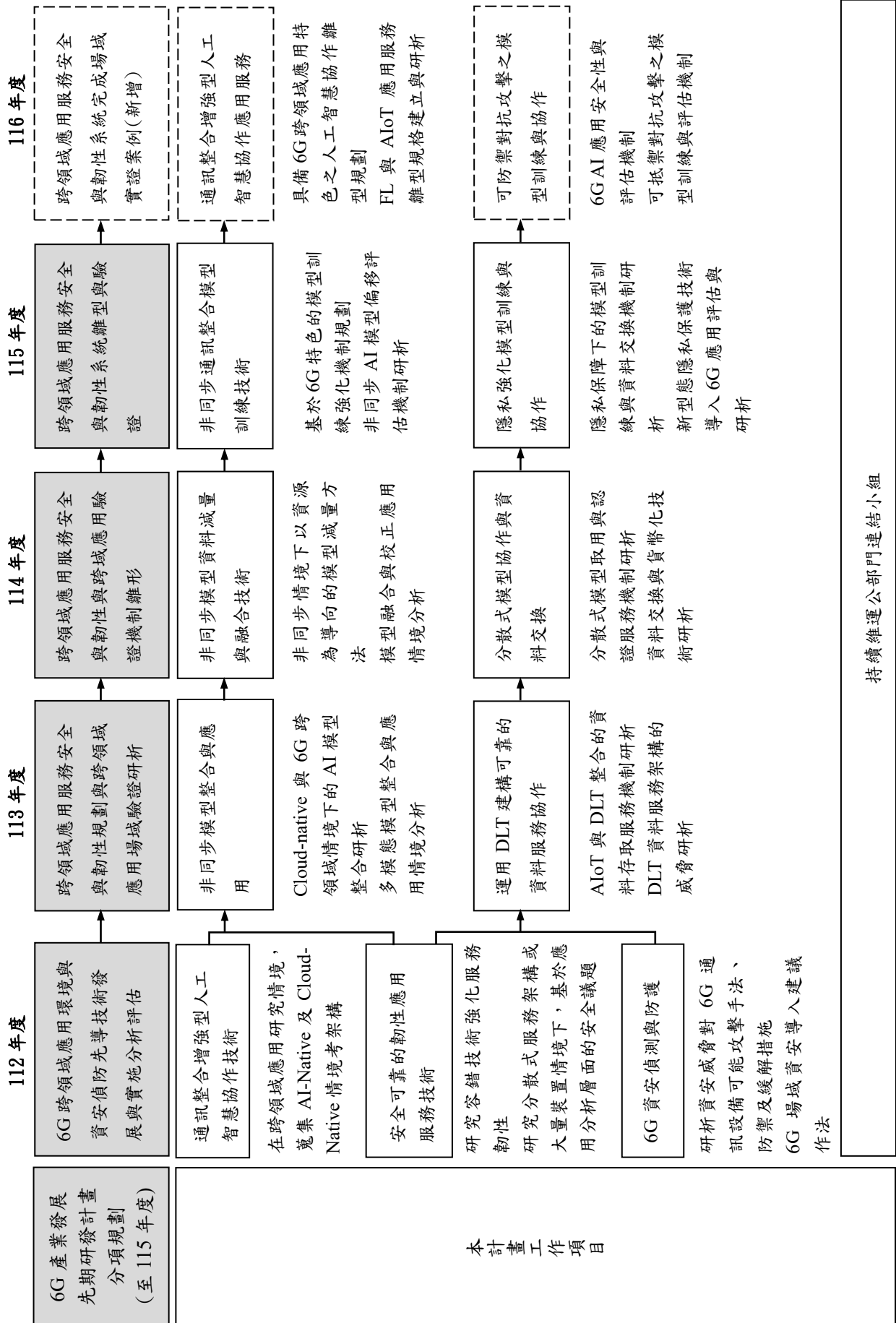
對應本計畫跨領域應用之規劃，則可參考 IMT-2030 的能力定義（如下圖 140），將結合 AI 應用與安全、隱私、韌性等特色，規劃跨領域應用在 6G 中應發展之技術與特色，提出以 DLT、AI 應用/安全、FL 等為主軸之技術研析與驗證。預期建構 6G 網路跨域與韌性應用產業生態，引領產業發展融合 AI、安全與隱私防護 6G 創新應用。



圖 140、IMT-2030 規劃中 6G 系統與應用應具備之能力

資料來源：請參閱附錄-參考資料^{8.2}

8.2 主要整理 ITU-R WP5D 第 44 次會議之相關討論與決議文件。(來源參考 <https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/Pages/default.aspx>)



未來 4 年執行之規劃，基於短期目標在資料隱私上的需求，故以在 6G Cloud-Native 特色之分散式應用時，資料由不同應用場域進行管理或透過端點雲進行近地端運算等需求，在此情境下優先考量以分散式帳本建立資料協作服務，以及基於此架構下的 AI 應用情境，如搭配 FL，進行各類型的資料分析服務、多模態模型之應用整合，如第 1 年的非同步模型整合與應用、運用 DLT 建構可靠的資料服務協作等，在第 2 年延伸第 1 年多模態模型的應用，持續進行非同步模型資料減量與融合，對 6G AI-Native 與 Cloud-Native 應用進行探討，作為後續模型管理、加值應用之參考，並於其中參考已制定/制定中的相關資料保護與應用標準，結合 DLT 進行資料貨幣化應用驗證，在第 3 年導入基於後量子密碼強化之通訊加密、資料保護技術，用以應對未來可能的量子攻擊，並透過場域的整合實證，探討後量子密碼應用可能帶來的副作用(如加密資料擴張等)，最後，雖然近期在可信任 AI 的立法與標準趨勢中，將會於近 2 年底定相關法規與驗測標準，本計畫預計在第 4 年納入 AI 安全與攻防測試的技術，對 6G 跨領域應用進行 6G AI-Native 與應用端的模型安全測試，並整理出基於 AI 法規與標準的 6G 調適建議與實證。茲將未來 4 年細部的執行內容與作法詳述於後：

一、跨領域應用服務安全與韌性規劃與跨領域應用場域驗證研析

(113 年度)

(一)非同步模型整合與應用

研擬 6G 應用體系下，於 Cloud-Native 整合 AI 應用時，遭遇連線異常狀態下時，AI 的非同步服務機制(包含訓練、推論)；以及結合分散式架構時(如 FL 等)，如何強化其應用架構，並對多模態模型的應用與整合進行探討。

(二)運用 DLT 建構可靠的資料服務協作

分析 AIoT/Massive IoT 情境下，結合 DLT 的資料整合管理與應用，包含隱私合規、存取機制、資料隱私/資安威脅等分析，以及在 6G 通訊環境下，遭受物理上的斷網或異常情形下，其韌性與回復機制之探討，並在隱私合規部分，納入歐美與臺灣個資相關法規調適與技術建議。

二、跨領域應用服務安全與韌性與跨域應用驗證機制雛形(114 年度)

(一)非同步模型資料減量與融合技術

規劃非同步情形下，對模型減量以強化通訊效率的機制，包含如何選取高效模型以及對其進行模型融合與校正，以其優化跨領域應用服務的品質與維持效率。

(二)分散式模型協作與資料交換

參考 ITU-FG DPM、ERC-20、ERC-721、ERC-1155 和 BEP-20 等相關規範或標準，探討 6G 跨領域應用情境下，模型與資料應用/交易等機制，探討未來可能的技術應用情境與商業化模式。

三、跨領域應用服務安全與韌性系統雛型與驗證(115 年度)

(一)非同步通訊整合模型訓練技術

基於 6G 標準雛型結合現有 AI 跨域應用情境，建立特色化的模型訓練與傳輸機制，或與實體通訊層整合，以達到傳輸效率強化，並基於 6G 標準雛型的需求，規劃應用模型(如 Self-attention、Large Multimodal Model、生成式 AI 等)或應用服務偏移監測機制。

(二)隱私強化模型訓練與協作

規劃基於後量子密碼學或同態加密技術之跨領域應用，以強化資料隱私達成可用不可見之效果，達成模型訓練與協作時的身分認證、隱私保護整合。



四、跨領域應用服務安全與韌性系統完成場域實證案例(116 年度)

(一)通訊整合增強型 AI 協作應用服務

以 6G 標準雛型與情境建構國內 AI 協作的場域示範，包含規劃資料、通訊、模型協作的整合情境與國際接軌。

(二)可防禦對抗攻擊之模型訓練與協作

對 6G AI 跨領域應用或 AI 核網應用，研析 6G 標準雛型以及如 ISO SC42、NIST、IEEE 等相關標準對 AI 風險管理與通訊整合應用之要求，建構基於 6G 導入 AI 整體安全之風險評估準則與攻防驗證。

**跨領域應用服務安全與韌性規劃與跨領域應用場域驗證研析(113 年度)**

項目	列考核項目	質化績效指標	量化績效指標
非同步模型整合與應用	Cloud-Native 與 6G 跨領域情境下的 AI 模型整合應用研析與國際觀測	研析 ITU、3GPP 等國際標準與國際大廠趨勢，提供有關單位作為參考	成果報告一份
	多模態模型整合與應用情境分析與實證	規劃多模態分析應用情境與 POC 驗證	技術規劃與實證分析報告一份
運用 DLT 建構可靠的資料服務協作	AIoT 與 DLT 整合的資料存取服務機制研析與國際觀測	研析 ITU、ISO、3GPP、等國際標準與國際大廠趨勢，提供有關單位作為參考	成果報告一份
	DLT 資料服務架構的威脅研析與實證	DLT 資料服務架構的威脅情境研析與 POC 驗證	技術規劃與實證分析報告一份

跨領域應用服務安全與韌性與跨域應用驗證機制雛形(114 年度)

項目	列考核項目	質化績效指標	量化績效指標
非同步模型資料減量與融合技術	非同步情境下以資源為導向的模型減量方法	研析 6G AIoT 國際標準與技術發展，進行技術規劃，提供有關單位參考	成果報告一份
	模型融合與校正應用情境分析與實證	模型融合與校正技術規劃與 POC 驗證	技術規劃與實證分析報告一份



分散式模型協作 與資料交換	分散式模型取用 與認證服務機制 研析	研析國際零信任 與認證技術，並 規劃應用於 6G AIoT 架構	成果報告一份
	資料交換與貨幣 化技術研析與實 證	參酌 ITU 等國際 標準進行情境規 劃與技術驗證	技術規劃與實證 分析報告一份
跨領域應用服務安全與韌性系統離型與驗證(115 年度)			
項目	列考核項目	質化績效指標	量化績效指標
非同步通訊整合 模型訓練技術	基於 6G 特色的 模型訓練強化機 制規劃	參考歐盟、美國 對可信任 AI 的 法規與技術規 範，研析 6G 生 態系下的技術對 接規劃	成果報告一份
	非同步 AI 模型 偏移評估機制研 析與實證	符合歐盟、美國 對可信任 AI 的 法規與技術規 範，研擬 6G AI 應用之評估機制 與實證	技術規劃與實證 分析報告一份
隱私強化模型訓 練與協作	隱私保障下的模 型訓練與資料交 換機制研析	以國際標準之資 料治理與法規遵 循為核心，融合 零信任框架，研 析 6G AIoT 隱私 技術應用與規劃	成果報告一份



	新型態隱私保護 技術導入 6G 應 用評估與研析	評估同態加密、 零知識證明等機 制導入 6G 應用 之可行性與實證	技術規劃與實證 分析報告一份
跨領域應用服務安全與韌性系統完成場域實證案例(116 年度)			
項目	列考核項目	質化績效指標	量化績效指標
通訊整合增強型 AI 協作應用服務	具備 6G 跨領域 應用特色之人工 智慧協作雛型規 劃	以 6G 場域情境 為核心規劃 AI- Native 下的協作 技術與雛型系統	成果報告一份
	FL 與 AIoT 應用 服務雛型規格建 立與研析	規劃符合聯合學 習與 AIoT 國際 標準與趨勢之框 架與機制，並進 行驗證	技術規劃與實證 分析報告一份
可防禦對抗攻擊 之模型訓練與協 作	6G AI 應用安全 性與評估機制	以隱私、AI 應 用安全為核心， 參考國際標準與 規範規劃技術指 引與建議	成果報告一份
	可抵禦對抗攻擊 之模型訓練與評 估機制	規 劃 6G AI- Native 下的對抗 攻擊攻防測試機 制與評估方法， 並提出實證	技術規劃與實證 分析報告一份

第四節 其他建議持續關注議題

IMT-2030 中提到對於量子技術提升可信度或強化安全之議題，然量子運算或類量子演算之普及與商用化發展與進程，尚待觀察，不過以現有普及運用之各類網路或通訊方式上的密碼學方法，在可見的未來，當大規模(Large-scale)通用型(Universal)量子電腦現世，將可破解當今所有公鑰密碼系統(Public-Key Cryptosystems)，包括行之有年的數位簽章。為抵抗量子計算帶來的威脅，PQC 應運而生，學術研究已有數十年。PQC 以數學演算法為基礎，可使用現有電腦與網路架構，不需額外基礎建設。美國政府正在制定 PQC 後量子密碼國家標準，NIST 於 2022 年 7 月已選出 4 項演算法^{8.3}，未來將成為後量子密碼國際標準，全世界通用。故將容易受到量子電腦衝擊的密碼系統，遷移到 PQC 的系統，是近年全球關注的重點，由於受影響密碼系統廣泛使用，相關加密協定之轉換，需要大量的時間與資源將既有系統逐步更新，此部分將從現有 5G 應用體系展開，本計畫可持續關注 PQC 與轉換/遷移相關作法與議題，協助產業升級既有 5G 應用安全並銜接至 6G 應用。

基於 6G 未來將具備 AI-Native 之核心特色，而 AI 發展與今年由生成式 AI 帶來新一波熱潮，相關國際組織與國家數年前即開始討論 AI 倫理與管理框架。國際組織與標準國家對於 AI 技術發展與應用展開擬定相關規範與準則之行動，期望人類運用 AI 增進社會福祉之際，也能努力防範或降低其可能帶來之風險。例如 NIST 於 2023 年 1 月正式推出「人工智慧風險管理框架 1.0 版」(Artificial Intelligence Risk Management Framework, AI RMF)，該框架由美國國會指示 NIST 制

8.3 NIST. (2022). PQC Standardization Process : Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates. Retrieved from <https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4>



定，目的在提供做為設計、開發、部署及使用 AI 系統之指南，降低應用 AI 技術的風險。

故對應未來 6G 相關核心網路以及跨領域應用將結合 AI 來展開，各國對於 AI 的風險管理與評估技術/標準，亦可考慮納入本計畫對 AI 導入 6G 生態系中之設計參考，以保障未來服務的安全性與可靠性。