109 年度

人工智慧導向資安共創技術計畫

合作研究計畫

《共享特徵選取演算法研發》

建議書徵求文件

財團法人資訊工業策進會

中華民國 109 年 3 月

109年度合作研究計畫建議書徵求文件

一、簡介

在工業4.0在帶領之下，傳統工具機業者邁向智慧機械，根據市調機構MarketsandMarkets的資料顯示，全球智慧製造市場規模預計到2023年將成長至2990億美元，2018年至2023年的複合年增長率（CAGR）為11.9%，智慧製造商機龐大。因應未來趨勢，製造業希望導入工業物聯網技術，設備資訊交換更顯重要。

由於工業控制系統缺乏資安考量，許多生產設備原本在獨立的系統與隔離的環境操作，在初期設計缺乏身份驗證和基本加密等防護功能。若內部網路遭入侵，常缺乏有效阻擋的機制，攻擊者在一點突破之後，可以輕易地進入生產製造系統的不同部分，如監視和管理生產程序的控制器，進而可能導致作業停擺、設備損害、財務損失、智慧產權被竊，以及大量影響人員健康和安全的風險，例如台積電因病毒於內網擴散損失52億、本田與雷諾車廠因勒索病毒產線被迫停擺等資安事件。

首先，各行各業大量的機台設備感測器透過物聯網都連上網路後，全部都將成為可能的攻擊目標，因為系統的安全性取決於最弱的點 (as strong as the weakest link)。傳統資訊安全僅止於電腦或行動終端設備與伺服器之間的通訊以及資料的保護，在物聯網快速導入各行各業之後，其數量規模更是比電腦設備急劇暴增，再加上設備或感測器在傳統設計上，並未考量傳輸的安全，強制規範符合資訊安全標準，於是這些便成為更容易下手的目標。其次，大量機台設備資料可能含有企業內重要的domain know-how，一旦被竊取將嚴重影響企業生存與競爭力。再者，由於 5G所能乘載的各項新穎服務更多，除了密切與個人身分與隱私相關，牽涉的層面也更廣，其所仰賴的人工智慧或是機器學習技術，萬一遭到入侵，竄改，則所影響的不只是個人，而是企業整體，甚至危害所有民眾。最後，除了資料必須確保不被竊取之外，也必須保證資料內容不會被竄改。

為了探討智慧製造物聯網的環境潛在的安全問題，本合作計畫（以下簡稱本計畫）將針對智慧製造物聯網場域進行分析與建模，然而智慧工廠環境下每個場域的機台設備與資料特性差異懸殊，通常需要大量人工標註資料，以供深度學習方法訓練有效的資料存取的模型，因此本計畫著重在，如何透過轉移學習(transfer learning)等方法，深入了解不同場域模型的差異，並且能測試模型自動轉移至新場域的效果，以節省大量人工標註的成本。

二、計畫目標

本計畫預計探討智慧製造物聯網場域進行機台設備資料存取的監控分析與建模，並進一步以深度學習方法訓練資料存取模型，透過轉移學習方法，根據不同場域的資料屬性的差異，進行模型自動轉移，最後測試轉移至新場域後的異常偵測效果。在智慧工廠資料存取建模方面，本計畫目標針對機台設備感測器等裝置進行自動化的資料存取紀錄和分析，以偵測可能的異常存取模式。本計畫預期研發的技術將可以針對已知網路協定的封包進行分析並建立模型，以提供異常偵測效果測試使用。透過上述流程，以其分析出不同場域資料存取模式的差異，並透過監控得知缺陷或弱點，提升整體環境的安全。

三、計畫範圍

本計畫應針對智慧物聯網場域建構一資料存取安全檢測模組，本計畫所產出之模組預計將提供制式的使用者或系統界接界面，接收來自主系統遞交的場域資料存取封包側錄資料檔，進行分析和建模後，產出分析結果以及場域資料存取模型。以提供其他系統進行整合與呈現。

四、預期成果

本計畫研發之模組，應可針對智慧製造物聯網環境之資料存取封包監控側錄資料檔案進行處理，並利用人工智慧相關技術進行分析，供研發人員或測試人員了解資料傳輸通訊協定的可能結構，建立適用於智慧工廠的測試資料。除此之外，本計畫針對不同場域的模型，應針對各自機台設備資料進行監控擷取與分析，以便了解場域資料屬性與潛在風險的相關性，以檢查安全方面的風險或漏洞。本計畫會有期中和期末報告各一份（含教育訓練），並且預期撰寫國內知名研討會或期刊論文一篇。

※前述成果如有專利構想或專利申請產出時，需注意專利申請之新穎性(novelty)。因凡經公開發表之研發成果，如擬申請專利，須於公開發表後 6 個月內完成，前述成果如是以論文方式公開發表，將無法取得大陸與歐盟等國之專利。

五、執行方式

本計畫預計將結合學界在理論面以及本會在資安弱點測試平台建置的實務面經驗，透過雙方相互合作討論的方式來進行，本計畫亦需提供教育訓練及經驗分享機制，藉此增進本會研究人員的專業能力，以提升本合作案成果之效益，相關執行方式步驟如下：

1. 完成相關文獻蒐集等先前技術整理。
2. 完成資料存取安全檢測模組系統架構規劃及架構程式編寫。
3. 完成資料存取安全檢測模組雛形系統，並完成系統功能測試。
4. 完成結案報告，驗證分析系統的正確性、成果品質以及教育訓練分享。

六、計畫期程及預估計畫總經費

計畫執行區間：109年01月01日至109年12月7日。

總經費：70萬元整(含稅)。

七、驗收標準（含教育訓練）

1. 期中、期末報告：分別預計於 109 年 8 月 30 日與 109 年 11 月 30 日完成期中與期末報告：
   - 期中報告的內容包含：系統架構的規劃方式及先前技術整理說明。
   - 期末報告的內容包含：系統操作行為檢測模組的研究成果、相關的功能驗證報告以及雛形展示。
2. 雛形系統：期末完成資料存取深度學習模型及轉移學習效果測試模組，包含執行檔、程式原始碼及檢測功能驗證。
   - 智慧工廠實際資料存取案例分析針對至少一個場域進行探討。

- 轉移學習部份需包含對另一個不同場域的設備資料進行深度學習模型自動轉移測試的實作。

3. 提供教育訓練：針對計畫成果移交、系統運作機制及操作說明等提供教育訓練。
4. 進度討論會議：每月召開一次進度研討會議。
5. 國內外知名研討會或期刊論文一篇。

八、技術能力需求

1. 資料分析與人工智慧相關背景：須瞭解網路系統運作原理，熟悉巨量資料分析技術，並具備機器學習等各項人工智慧相關技術模組開發經驗，能掌控本計畫研發所需核心技術。
2. 相關計畫參與經驗：熟悉深度學習運作原理，了解轉移學習運作原理，並具相關領域研究論文發表及計畫執行經驗。
3. 其他：如熟悉 C/C++、Python、一般深度學習架構如 Keras/TensroFlow/PyTorch 等框架的運作與程式撰寫。