

一、前言

隨著物聯網普及，更多的裝置都具備聯網功能，伴隨而來的是巨量的累計資料，過去數據傳輸至中央雲端系統進行運算分析，然而在大數據時代下，無法僅仰賴中央運算系統，更需要的是低延遲、及時的運算能力，邊緣運算(Edge Computing)即能提供這樣的服務。邊緣運算帶動人工智慧的應用與運算更加快速，同時卻也讓邊緣設備的監控與防護變得更加困難，本篇文章將帶您一同了解邊緣運算及其衍生的資安風險與挑戰。

二、什麼是邊緣運算

邊緣運算是將部分數據儲存及運算功能移出中央雲端(數據)系統，進而在實際生成數據的裝置上或比中央系統更近的地方，直接進行運算，大幅降低過去數據必須先回傳至中央系統所耗費的時間，促使運算變得更加及時，可以快速提供決策者相關數據。邊緣運算主要應用實例包括：自駕車、智慧零售、智慧工廠等。

三、邊緣運算衍生資安風險

1. 擴大的攻擊面

大多邊緣設備無法具備像中央雲端系統強大的資安防護能力，數據不再集中於一處時，駭客就更有可能多點侵害這些防護力相對較弱的邊緣設備。

2. 身份驗證

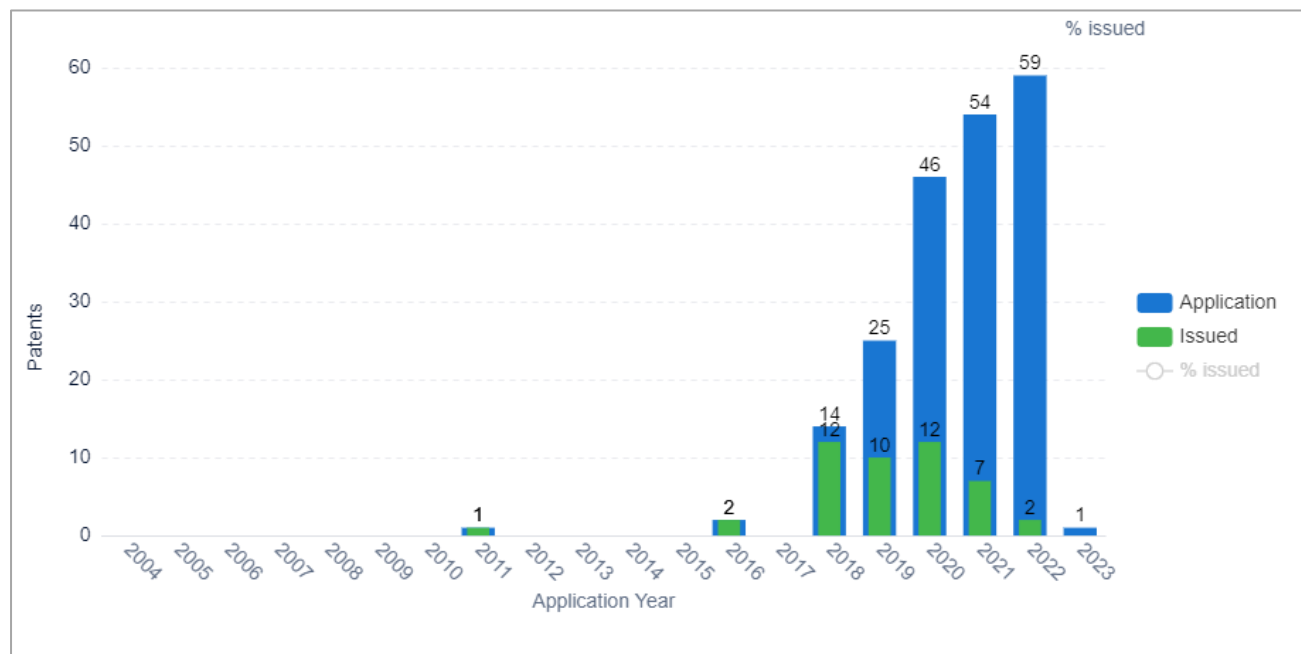
邊緣設備通常由不具備 IT 或資安背景的人所使用，以及設備上的密碼控管通常較不嚴謹，導致邊緣設備極有可能輕易受駭客入侵。

3. 數據蔓延

聯網設備只會越來越多，導致企業需要管理的範圍擴大，監控也將變得更加困難。隨著聯網設備的增長，物聯網流量也將增加延遲。

四、邊緣運算及資通安全專利技術布局趨勢

由下圖 1 可見，與邊緣運算相關的資通安全專利，於 2018-2022 逐年上升，並且穩定成長。



(圖片來源：[PatSnap](#)，檢索日期：2023/02)

圖 1、與邊緣運算相關的資通安全專利技術申請趨勢

其中，於此領域下被引用次數前 5 名的專利如下表 1，被引用的次數越多，代表此技術為該領域核心技術。由下表 1 可見，5 件專利之申請人除了個人外，分別來自 OSRAM 和 Intel。OSRAM 之專利為光學雷達感測器，感測器是支撐物聯網的核心技術，並隨著科技進步，發展為具備邊緣運算功能之智慧型感測器(相關文章：[《支撐物聯網時代的核心技術：智慧型感測器》](#))。Intel 之專利為有效管理多件節點(感測器)進行邊緣運算並穩定傳輸量能之方法，以自駕車為例，一部自駕車同時搭載多組感測器以蒐集數據並因應駕駛周圍的環境變化，如何有效控管多組感測器並提供駕駛正確的行駛判斷，是一項非常重要的技術。

表 1、被引用次數前 5 名專利

公告號	專利名稱	申請人	被引用次數
US20200284883A1	Component for a lidar sensor system, lidar sensor system, lidar sensor device, method for a lidar sensor system and method for a lidar sensor device	OSRAM GmbH	196
US20210144517A1	Multi-entity resource, security, and service management in edge computing deployments	Intel Corporation	112

US20200311559A1	Optimized decision tree machine learning for resource-constrained devices	Chattopadhyay, Rita (US); Bansal, Rajesh (SG); Ma, Yuming (US); Ganguli, Mrittika (US)	89
US20200229206A1	Methods and devices for wireless communications	Intel Corporation	83
US20200027096A1	System, business and technical methods, and article of manufacture for utilizing internet of things technology in energy management systems designed to automate the process of generating and/or monetizing carbon credits	COONER, JASON RYAN (US)	58

(資料來源：[PatSnap](#)，檢索日期：2023/02)

與邊緣運算相關的資通安全專利，技術應用概念如下圖 2，感測器為蒐集數據的根本，隨著人工智能與機器學習技術進步，發展為兼具邊緣運算功能的智慧型感測器。如同前述，當每項邊緣設備都具備運算能力，而不一定要透過中央運算系統執行時，相對的是提供駭客更大的攻擊面，因此如何提升邊緣設備控管信息安全及防護惡意軟件的能力，是現今重要的發展趨勢。



(圖片來源：台灣技術交易資訊網繪製)

圖 2、與邊緣運算相關的資通安全技術應用概念

五、結語

5G 技術的發展，也將加重物聯網、邊緣運算的資安風險，強化端點及網路防禦，是現今企業必須重視的議題。除了資安防護技術的提升，建立員工資訊安全知識，亦為迎接資安防護戰的一項重點，面對資安攻擊雖然無法百分之百防禦，但企業可從其他角度補強防禦能力。

參考資料

1. https://www.itri.org.tw/ListStyle.aspx?DisplayStyle=18_content&SiteID=1&MmmID=1036452026061075714&MGID=777744451502402317
2. <https://www.section.io/blog/security-challenges-network-edge/>
3. <https://www.tutorialspoint.com/edge-computing-security-risk-and-challenges#>
4. <https://www.simplilearn.com/edge-computing-security-risk-and-challenges-article>
5. <https://www.techtarget.com/searchdatacenter/definition/edge-computing>
6. <https://www.ithome.com.tw/voice/151578>
7. 專利資料來源：[PatSnap](#)