

科技部

111 年度大專學生研究計畫申請書

一、綜合資料：

申請人 【學生】	姓 名	洪胤勛		身分證號碼	N126356072
	就 讀 學 校、 科 系 及 年 級	暨南國際大學 資訊工程學系 三年級		電 話	0965598275
	學 生 研 究 計 畫 名 稱	可延展式與容錯性 WebAPI 安全管制機制之設計			
	研 究 期 間	自 111 年 7 月 1 日至 112 年 2 月底止，計 8 個月			
	計 畫 歸 屬 司 別	☐ 自然司 ☒ 工程司 ☐ 生科司 ☐ 人文司(含科學教育領域)			
	研究學門代碼及名稱	E4003 計算機網路與網際網路			
	上年度曾執行本部大專學生研究計畫	☐ 是（計畫編號：MOST — — — — ） ☒ 否			
指導教授	姓 名	吳坤熹		身分證號碼	S120642448
	服 務 機 構 及 科 系(所)	國立暨南國際大學 資訊工程學系			
	職 稱	副教授		電 話	(049)2910960 Exit 4736
補助經費	項 目	金 額	說 明		
	研 究 助 學 金	48,000 元	每月補助研究助學金新臺幣 6,000 元，8 個月計新臺幣 48,000 元。		
	耗材、物品、圖書及雜項費用	0 元	依研究計畫實際需求擇優補助，每一計畫最高以補助新臺幣 20,000 元為限。		
	合 計	48,000 元			

表 C801

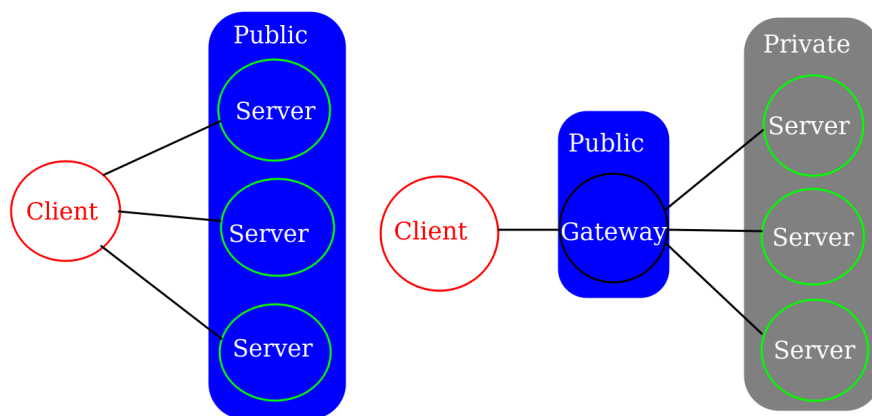
系 主 管 姓 名：陳恒佑
(學生就讀學校)

二、研究計畫內容（以 10 頁為限）：

（一）摘要

在一個分工的時代，工程師也要懂得如何分工。在軟體工程裡面，有個專有名詞叫做 API (Application Programming Interface)。他是一個溝通的介面，旨在讓工程師們專心在他們的任務，而不需要管理其他層面的問題。比如說一個人用電腦時，他只要知道鍵盤、滑鼠可以輸入資料，螢幕可以輸出結果，但他並不需要去知道電腦是如何運作的。如果是網頁的開發，通常會分為前端和後端，前端負責設計使用者介面，後端負責資料的儲存，他們溝通的介面，又可稱為 WebAPI。

（二）研究動機與研究問題



圖一、傳統 Web Server 圖二、WebAPI Gateway

研究動機

在使用網頁時，通常使用者 (client) 會需要去 WebAPI 服務端提取資料 (也就是 server 端)。當使用者需要多筆資料，而那些資料可能是由不同的服務端所提供的，那他形成的架構就會像(圖一)。但這架構會造成一個大問題，每個服務端都必須要有一個公用的 IP 地址，也就表示所有人可以直接連到服務端。尤其在 IoT 的佈建當中，許多的感測器是由外包廠商負責建置，再透過公開的 4G 網路傳回伺服器。IoT 設備由 4G 取得的是浮動的 IP 位址，因此實務上伺服器都必須擁有固定的公開 IP 位址，以讓 IoT 設備傳回資料。如果有心人士想竊取伺服器的資料，

或是想讓伺服器癱瘓，那這種架構極有可能會讓有心人士達成他們的目的。

於是後來有了 Gateway (圖二) 這架構。Gateway 扮演了使用者連到服務端間的中繼站，使用者需要的資料都間接透過 Gateway 取得，服務端要給使用者的資料也都透過 Gateway 傳送。公用的 IP 地址只需要 Gateway 這台電腦擁有，真正在服務的服務端可以只使用私用 IP 地址。這解決了剛剛所提到的問題，服務端不再需要暴露在所有人都可以直接連線的狀況。除了上述的好處之外，Gateway 還能讓服務端的管理者清楚知道當前有哪些電腦正在對外提供服務，並把沒在提供服務的電腦給關機，減少了被入侵的機會。

研究問題

雖然上述的架構解決了把服務端暴露在公用 IP 的環境，但相對地，也讓風險全部都在 Gateway 上，只要 Gateway 停止運作，那麼使用者也沒辦法正常使用我們的服務。為了解決此問題，此研究將使用 Gateway 與 Kubernetes 搭配，讓停止運作的 Gateway 再次重啟。

現在開源的 Gateway 也有很多，此研究也將對各種 Gateway 進行效能上的分析與比較。

(三)文獻回顧與探討

Express Gateway

Express 是一個開源的項目，使用 node.js 來編寫程式。它提供了動態且集中式的管理系統，還提供了使用者和憑證管理 [1]。

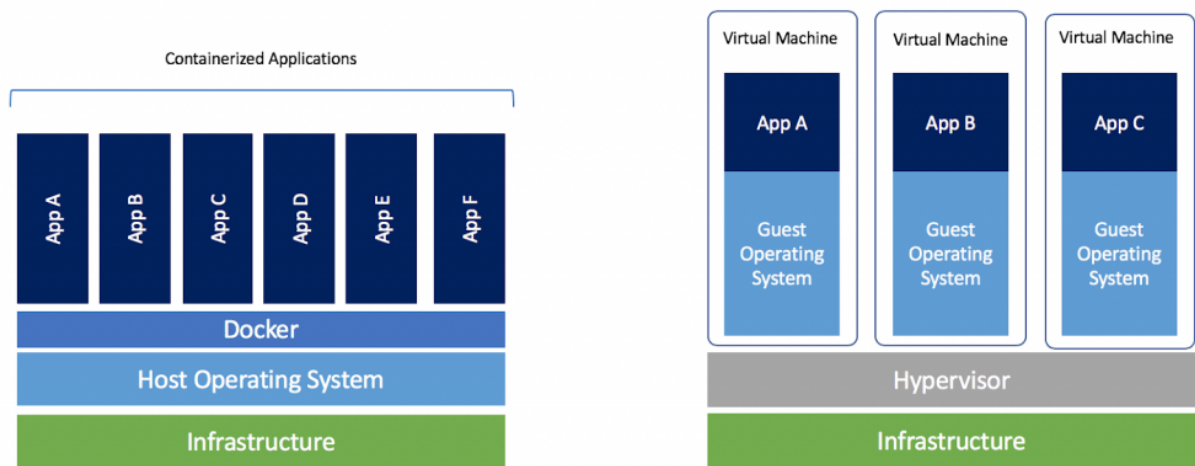
API Umbrella

API Umbrella 是一個開源的軟體，使用 ruby 來編寫程式。他讓 API 創建者和使用者更容易去使用。創建者可以專心在開發 API 上，而其他的管理(像是限速、訪問控制)則交給 API Umbrella。而使用者可以只透過單一端點訪問到服務端所有的 API，且標準化了訪問的流程 [2]。

Kong API Gateway

Kong API Gateway 使用 lua 編寫程式，其軟體又分為開源版本和企業版本。在本節所提及的三個 Gateway 中，它最為社群所信賴。Kong 提供了大量的插件，包含了使用限速、用戶端的認證，以及客製化的 log 形式。建立者還可以透過 lua 來編寫 log 所要輸出的結果[3]。

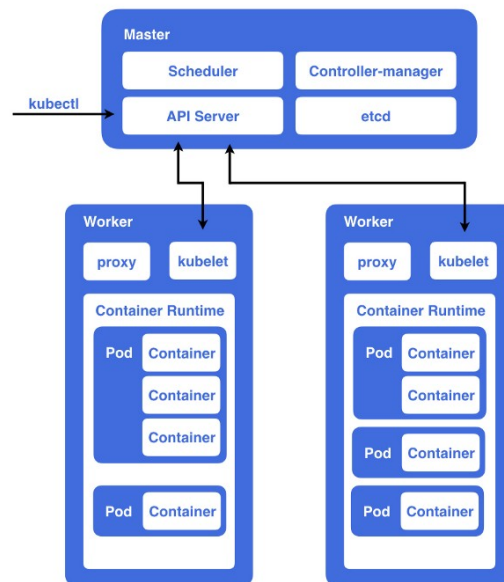
Docker



圖三、Docker vs. VM [4]

Docker 使用 GO 語言開發，為開源軟體。Docker 的基本單位為 container，其原理與虛擬機（VM）類似，但卻比虛擬機更為輕巧，更能夠快速地建立起來。傳統的虛擬機著重在將硬體設備給虛擬化，而 container 則著重在將作業系統給虛擬化。如(圖三)所示，左邊為 container 的架構，右邊則為傳統的虛擬機。我們可以看到，右邊的虛擬機可以把一台電腦的硬體支援分配給多台虛擬機，但每台虛擬機都需要有作業系統在上面執行。左邊的 container 一樣是把硬體資源分配給 container，但值得注意的是，每個 container 並不需要再架起一個作業系統，這也是為什麼 container 比起虛擬機更為輕量，更能夠快速建立起來的原因 [5]。

Kubernetes



圖四、Kubernetes 架構 [6]

Kubernetes 又稱為 K8s，使用 GO 語言開發，且為開源軟體。由 Google 設計出來，現在已屬於 Cloud Native Computing Foundation。K8s 中，一個基本單位為 Pod，Pod 裡面可以有一個或多個 container，但通常只會有一個。在運行 K8s 時，有兩個主要腳色，如(圖四)所示，為 Master 和 Worker，Master 和一個或多個 Worker 組合起來就稱為 Cluster。

使用者會在 Master 端下達指令，告訴 K8s 我們要架起服務的需求共要幾個 Pod。Master 則會根據 Worker 的狀態，來決此 Worker 要分配幾個 Pod。K8s 中還有一個物件為 Deployment，他的工作是保持 Pod 的數量，當 Pod 若因意外故障而少於預期的數量，Deployment 則會啟動新的 Pod，讓 Pod 維持在一定的數量[6][7][8]。

(四)研究方法及步驟

步驟一：

此實驗將先在單一台電腦上使用 Docker 執行單一個 API Gateway 的 container，確認單一個 container 能夠順利運行。

此步驟將會嘗試多的開源的 API Gateway，包含 Express Gateway、API Umbrella、Kong API Gateway。

在成功運行 container 後，針對不同的 API Gateway，確認他們能否照著需求去開創。

步驟二：

準備三台電腦，這三台電腦會用來運行 K8s Cluster。

步驟三：

分配三台電腦，讓他們去運行一個 K8s 的 Cluster，其架構如(圖四)所示，會有一台 Master 來管控 Cluster 裡佈署狀態，另外兩台為 Worker，為真正運行 Gateway 的地方。

步驟四：

在建立完 K8s Cluster 且確認 Master 與 Worker 能正常運作後，把 Gateway 透過 Master 來佈署到我們的 Cluster 上。

此步驟將會嘗試多的開源的 API Gateway，包含 Express Gateway、API Umbrella、Kong API Gateway。

在佈署完成後，針對不同的 API Gateway，確認他們能否照著需求去開創。

步驟五：

針對每個 API Gateway 進行量測，量測內容包含他們的吞吐量、單個 API 請求的回應時間。

在測量完成後，將對各個不同的 API Gateway 進行比較。

(五)預期結果

(一) 此計畫將會搭建出 API Gateway，並讓使用者的連線都須透過此 Gateway。

(二) 使用 Gateway 與 K8s 做搭配，並使用多台電腦，做到動態的負載，且最大限度地提升各電腦的使用效率。

(三) 此計畫將測量各開源的 Gateway，比較他們之間在電腦效能上的使用、對於大流量的表現。

(六)參考文獻

- [1] "github," ExpressGateway, [Online]. Available:
<https://github.com/ExpressGateway/express-gateway>.
- [2] "github," National Renewable Energy Laboratory, [Online]. Available:
<https://github.com/NREL/api-umbrella>.
- [3] "github," Kong, [Online]. Available: <https://github.com/Kong/kong>.
- [4] alfredkosasihh, "ithelp," October 2020. [Online]. Available:
<https://ithelp.ithome.com.tw/articles/10250841>.
- [5] "wiki," 12 10 2013. [Online]. Available: <https://en.wikipedia.org/wiki/Docker>.
- [6] C.-W. Hu, "kubernetes-basic-concept-tutorial," July 2019. [Online]. Available:
<https://cwhu.medium.com/kubernetes-basic-concept-tutorial-e033e3504ec0>.
- [7] "Kubernetes", June 2014. [Online]. Available: <https://en.wikipedia.org/wiki/Kubernetes>.
- [8] M. Lukša, "Kubernetes in Action", 2nd Edition, Manning, February 2020. [Online].
Available: <https://www.manning.com/books/kubernetes-in-action-second-edition>.

(七)需要指導教授指導內容

吳坤熹老師是本校網路通訊的專家，在 IPv4 與 IPv6 的轉移機制提供了許多的貢獻及論文。吳老師長年與埔里基督教醫院進行多年的合作計畫，協助醫院進行網路安全的架構提升，以及 API Gateway 的建置與容錯機制設計，對於醫院在實務上的網路需求有足夠的解析。此計畫，教授將提供實驗的背景理論以及實驗器材。

表 C802

三、耗材、物品、圖書及雜項費用：

大專學生研究計畫指導教授初評意見表

一、學生潛力評估：

洪胤勛同學非常的好學，常在課堂提出自己的問題，沒弄懂的地方總會打破砂鍋問到底，學業更是名列前茅，目前總排名為全班第二名。除了在課堂表現得不錯外，在課外，也積極的參與國內外的活動。曾代表學校，參加了中南部的 NCPC (National Collegiate Programming Contest) 程式競賽，還參加過新加坡超級電腦中心舉辦的 RDMA 黑客松 (Remote Direct Memory Access Hackathon)，在來自歐亞各國共 41 隊伍中，獲得了第三名的佳績。此外，在 GitHub 社群上，也經常參與討論，並對一些專案有不少貢獻。不論在課內或課外，都非常優秀。

二、對學生所提研究計畫內容之評述：

洪胤勛同學的研究計畫中，Gateway 不論對於資安的防護，或是對於公開 IP 地址的保護都極為重要。而 Gateway 搭配上當前的虛擬化技術和 Kubernetes，可以達成高效率的搭建與動態的分配。期待在研究完成後，能夠把這套機制技術轉移給相關的業界，協助強化其 Web 服務的資安架構。

三、指導方式：

此實驗將先建立學生對於 Gateway 與 K8s 的基礎理解，在之後將與學生對於效能與效率偵測上做進一步的探討。

四、本人同意指導學生瞭解並遵照學術倫理規範；本計畫無違反學術倫理。

指導教授簽名：吳坤熹

2022 年 2 月 16 日