二、研究計畫內容（以 10 頁為限）：

(一) 摘要

在未來的網路安全發展中，SIEM（Security Information and Event Management）系統將扮演關鍵角色。SIEM 系統透過整合即時監控、安全事件分析與集中化日誌管理[15]，為企業提供全面的安全態勢感知。在工業 5.0 強調 AI 與人類協作的背景下，整合 SIEM 與進階威脅偵測變得尤為重要。特別是針對 SQL 注入攻擊、XSS（cross-site script）及 DDoS（distributed denial-of-service attack）等威脅，SIEM 系統需要具備更強大的分析與應對能力[13][14]。

本計畫聚焦於將 DDoS 攻擊偵測與防禦機制整合至 SIEM 系統中，建立一個更全面且高效的威脅管理平台。再計畫書撰寫期間，我們發現從過去的案例顯示，美國電廠 sPower 曾因 DoS 攻擊導致電力系統短暫失效[18]，而 ChatGPT AI 服務也曾因 DDoS 攻擊而中斷[1]。這些事件凸顯了在 SIEM 系統中加入專門的 DDoS 偵測與防禦機制的重要性。透過 SIEM 系統的集中管理能力，可以更快速地發現和應對 DDoS 攻擊，並與其他安全防禦措施共同運作。

本計畫擬開發一個整合至 SIEM 架構的 DDoS 偵測模組。該模組採用深度學習技術分析網路流量並辨識異常模式，其偵測結果將即時饋入 SIEM 系統進行集中分析與管理。SIEM 系統負責整合日誌數據、產生即時警報，並追蹤攻擊來源。當偵測到 DDoS 攻擊時，SIEM 系統可立即執行應對措施，如中止可疑 IP 連接或調整頻寬配置。本計畫將使用 CIC-IDS-2017 和 CIC-IDS-2019 等資料集訓練 AI 模型，並將傳統偵測方法與機器學習技術結合，形成多層次的安全防禦機制。這些防禦機制都將統一由 SIEM 平台進行管理與監控。透過將 SIEM 系統納入 DDoS 偵測架構，本計畫希望能提升工業 5.0 的網路服務穩定性，為數位化生態提供一個高效且可擴展的安全解決方案。

關鍵字：SIEM 系統、DDoS、工業 5.0、AI、深度學習、AI 模型訓練

(二) 研究動機與研究問題

有許多企業採用防範 DDoS 攻擊的機制，例如使用反向代理服務、限制相同 IP 位址的訪問次數，以及限制每個 IP 位址的請求數量[17]。然而即使採取這些措施，當遇到大規模攻擊時，現有機制仍可能導致嚴重的服務中斷。為了減少這類問題的發生，本計畫嘗試使用 CIC-IDS2017、CIC-IDS2019 以及通過攻擊工具取得攻擊特徵，進而用於訓練 CNN-GRU 模型，以強化網路偵測系統的偵測能力。

本計畫預期採用 CNN-GRU 方法訓練模型[19]，透過深度學習技術，系統能夠偵測出未曾見過的 DDoS 攻擊模式。使用訓練後的模型進行攻擊辨識時，主要挑戰包括如何有效進行模型訓練、以及在訓練完成後對模型進行改良，以降低誤判率。主要提升 AI 模型的效率，因為在實際網路監控中，系統需要快速做出準確判斷。

(三) 文獻回顧與探討

根據研究動機與研究問題，本計畫將首先探討 SIEM 系統的基本原理及其在現代網路安全防禦中的作用，並進一步分析 DDoS 攻擊的常見手法。為了充分理解這些攻擊，本計畫將回顧目前已知的各類 DDoS 攻擊方式；接著將討論如何進行模型訓練，以有效辨識並防範這些攻擊；最後，本計畫將探討 SIEM 系統如何協助收集與分析日誌資料，實時監控並應對安全事件，特別是在 DDoS 防禦中的實際應用。

3.1 SIEM 系統在網路安全中的應用

SIEM（Security Information and Event Management）系統主要用於協助網路安全管理員設計與實施安全策略，並管理來自各種不同來源的安全事件。其核心功能是集中監控、分析和回應網路中的安全事件，從而增強整體網路防禦能力[12]。

3.1.1 SIEM 系統的基本架構

SIEM 系統由多個元件組成，每個元件都有其特定的功能，共同工作以達到最佳的安全效果。主要元件描述參考表一[12]。

表一、SIEM 基本元件描述[12]

元件	描述
設備來源	從各種網路設備（如防火牆、入侵檢測系統、路由器等）收集的安全事件和日誌數據
日誌收集	負責集中收集來自不同設備和應用的日誌數據
解析與正規化	將收集到的原始日誌數據進行解析和正規化處理，使其格式統一，便於後續分析與處理
規則引擎	使用預定的安全規則來分析日誌數據，從中分析潛在的安全威脅與異常
日誌保存	對收集到的日誌數據進行保存，確保數據的完整性和可追溯性，並便於未來查詢與審計
事件監控	實時監控網路中的各種安全事件，並根據設定的規則和策略做出即時通報

這些元件共同運作，能有效提高對網路安全事件的辨識、分析與應對能力，是現代網路防禦中的關鍵組成。

3.1.2 SIEM 的主要應用場景

SIEM 系統的應用範圍廣泛，涵蓋多種網路攻擊的偵測與防禦。SIEM 系統可以透過監控網路流量，分析流量異常，並及時發出警報，協助防禦措施的啟動[12]。

3.1.3 SIEM 的攻擊偵測能力

SIEM 系統可以用於偵測諸多類型的攻擊，如暴力破解、內部威脅、惡意程式碼等，並提供相應的應對策略。透過整合各種應用，SIEM 系統能夠提供全面的安全監控，集中檢視潛在威脅，即時威脅分析回應並獲取進階威脅情報，還有提供稽核和報告法規合規性，使得在監控使用者、應用程式和監控上更透明[20]。

3.1.4 DDoS 偵測與 SIEM 結合的優勢

將網路分析紀錄與 SIEM 儀表板整合，提供對 L3/4 流量(OSI 模型的網路層以及傳輸層)和 DDoS 攻擊的可見度，可以協助維護全面的威脅偵測系統，並更容易的向監管機構證明合規性。透過網路分析紀錄整合 SIEM 系統能夠更有效地應對各種網路攻擊[21]。

在此基礎上，本計畫預期將融合入侵檢測系統（Intrusion Detection System, IDS）與 AI 技術，並將其整合進 SIEM 系統中，以強化 DDoS 攻擊的偵測與防禦。具體而言將 IDS 作為設備來源，提供來自網路中的安全事件與日誌數據。數據將進一步進行預處理與正規化後，交由 AI 模型進行深入分析。

事件監控與規則引擎將在此過程中共同工作，根據 AI 的辨識結果動態調整防禦策略。例如在偵測 DDoS 攻擊時，SIEM 系統會立即發出警報並啟動防禦措施，中止攻擊源 IP 的連接或限制帶寬，以減少服務中斷的風險。

3.2 DDoS 攻擊研究現狀

DDoS（distributed denial-of-service attack）攻擊是一種通過大量分佈在全球的受控設備發動的網路攻擊，目的是讓目標系統或服務因為大量無效的請求而無法提供正常服務。隨著網路的快速發展和物聯網（IoT）的普及，DDoS 攻擊的威脅逐漸增強。DDoS 攻擊已經從簡單的流量洪水攻擊，演變成更加多樣化和隱蔽的形式，如應用層攻擊和複合型攻擊，這些攻擊方式常常難以被傳統的防禦系統辨識[2][9][10][11]。

3.2.1 現有的 DDoS 防禦技術

目前防禦 DDoS 攻擊的技術已經發展出多層防禦體系，像是反向代理、防火牆設定、流量分析、分佈式檢測與吸收，具體的詳細防禦方式如表二。

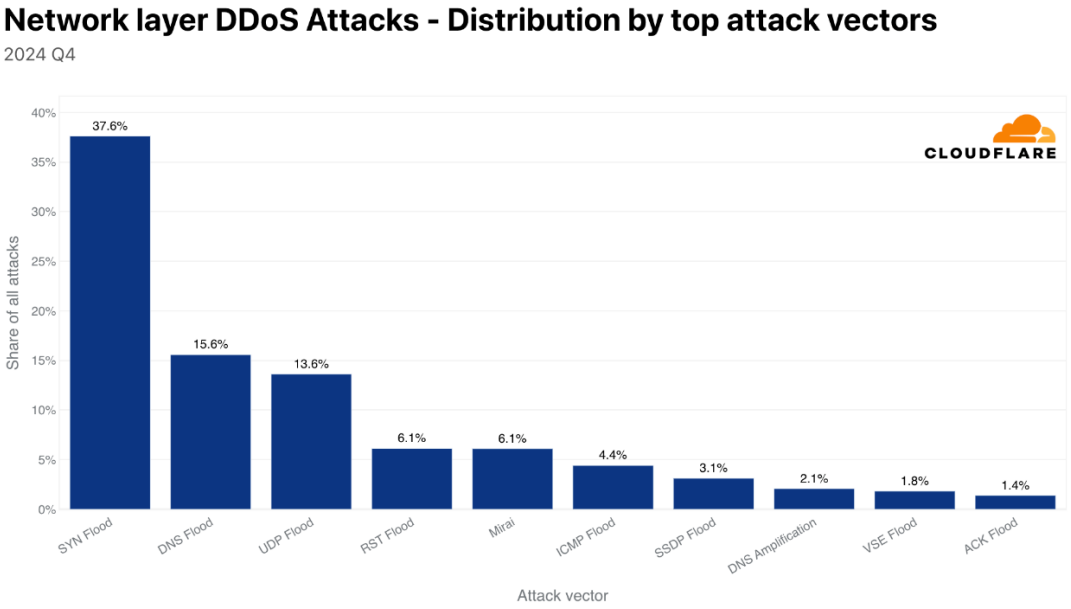
表二、現有的 DDoS 防禦技術[3][8]

防禦手法	做法
反向代理	反向代理服務可以作為網路和內部服務之間的中介，將來自外部的請求引導至代理伺服器，利用其大規模的基礎設備來吸收和過濾流量，減少目標伺服器的負擔
防火牆設定	通過設定預定規則來阻止不正常的流量
流量分析	基於流量特徵的模式識別、統計分析和機器學習方法可以檢測到 DDoS 攻擊
分佈式檢測與吸收	利用全球分佈的基礎設備，將攻擊流量吸引到全球不同節點，從而分散攻擊流量並降低本地網路的壓力

現有的 DDoS 防禦技術已經有一定的進展，但透過計畫書撰寫的期間，我們藉由文獻蒐集也發現 DDoS 的相關防禦議題仍然存在可以進一步改善的空間。首先面對大規模分佈式 DDoS 攻擊時，傳統的流量過濾技術可能會過載，無法有效處理大量的攻擊流量。其次應用層攻擊和複合型攻擊逐漸增多，這些攻擊不容易被傳統的防禦技術檢測出來。再者許多防禦系統在偵測到攻擊後，無法即時做出反應或應對策略仍不夠完善，導致服務中斷。

3.2.2 現有的 DDoS 常見攻擊

本計畫製作的工具需要偵測各種 DDoS，因此需要先知道當前有的 DDoS 的各項攻擊。DDoS 有多種攻擊手法[3]，因此需要先辨識是哪類型的 DDoS 攻擊，根據圖一可以看到 2024Q4 季度的網路層常見攻擊手法，如頻寬消耗型有 UDP Flood 攻擊、ICMP Flood 攻擊，資源消耗型有 SYN Flood 攻擊、LAND 攻擊、CC 攻擊、HTTP Flood 攻擊、DNS Flood 攻擊，這些都是比較常見的一些 DDoS 攻擊，各個攻擊手法都略有不同，目的都是癱瘓服務。



圖一、CloudFlare 2024Q4 網路層 DDoS 攻擊佔比分布[9]

頻寬消耗型攻擊其目的是通過傳送大量無效的「流量」的數據請求，堵塞被攻擊的伺服器頻寬，使其達到飽和狀態，讓正常用戶無法進入，甚至造成網頁當機癱瘓[4] 。資源消耗型攻擊使用「請求」耗盡目標系統的資源，使得伺服器不斷的反覆無效運作，最後導致整台主機運算資源被耗盡，由此方法來達成 DDoS 的攻擊。

面對於 UDP Flood 攻擊（User Datagram Protocol floods）[3]，UDP 封包不需要握手進行驗證，當大量 UDP 封包送給伺服器端時，將會使得頻寬過載，結果導致伺服器的服務無法請求；UDP 封包進行攻擊時，攻擊者會先收集受害系統的 IP 地址和端口，並使用殭屍網路等工具，向目標系統發送大量的 UDP 封包，因此受害的系統沒有辦法處理這些封包，會回傳大量的 ICMP 封包給送封包進來的主機，攻擊者會偽造自己的 IP 位址，此時 ICMP 封包不會真正回傳給發送封包進來的主機，受害系統一直接收到這些大量封包後，受害系統的網路資源將會消耗殆盡，進而導致系統癱瘓。

在 ICMP Flood 攻擊中，攻擊者會傳送大量的 ICMP 回應請求封包，傳送的封包內容是 ICMP 的各種訊息，持續傳送 ICMP 封包直到目標裝置無法處理所有的請求，從而消耗裝置的資源，導致正常流量無法進入受害系統[7] 。

3.2.2 現有的 DDoS 攻擊工具

DDoS 有多種攻擊手法[3]，因此需要先知道目前已經存在的攻擊工具，通過了解現有工具的特性與應用場景，才能設計有效的防禦和檢測系統，攻擊工具包含 LOIC(Low Orbit Ion Cannon)、HOIC(High Orbit Ion Cannon)、Mirai、Slowloris、Xerxes 等，具體攻擊工具對應 OSI 分層參考表三，各個攻擊手法都略有不同，目的都是癱瘓服務。

表三、DDoS OSI 分層攻擊工具分類[6]

Layer	工作內容	攻擊常見工具	攻擊功能
Application 應用層	應用程式網路程序	Slowloris, HOIC	HTTP 請求攻擊
Presentation 展示層	資料展示和加密		
Session Layer 工作階段層	中間主機通訊	R-U-Dead-Yet	維持 Session 開啟
Transport Layer 傳輸層	端點對端點和可靠性	LOIC, XOIC	TCP/UDP 洪水攻擊
Network Layer 網路層	路徑判定和邏輯定址	LOIC, Mirai, Hulk	使用 Bot-Net 發起大規模流量攻擊
Data Link Layer 資料鏈結層	實體定址	Ettercap	ARP 欺騙與中間人攻擊

Physical Layer 實體層	媒體、訊號和二進位傳輸		

現有的攻擊工具雖然無法完全模擬真實攻擊情況，但它們仍然可以作為測試防禦系統的基礎工具，用於檢驗系統是否具備應對已知攻擊模式的能力。然而，面對現代 DDoS 攻擊日益多樣化的特性，單純依賴這些工具可能會導致偵測系統的適應性不足，無法應對新型或變異的攻擊模式。

因此本計畫的重點在於利用 AI 技術強化 DDoS 偵測系統的能力，並將其與現有 SIEM 系統相結合，實現更加精確且快速的威脅辨識與通報。我們並不以改善攻擊模擬為基礎，而是專注於如何透過深度學習技術分析多樣化的網路流量，並結合傳統防禦機制，提升系統對於已知及未知攻擊的辨識能力。

3.3 深度學習在 DDoS 偵測中的應用

隨著 DDoS 攻擊手法的日益多樣化與複雜化，傳統的基於規則的偵測方法已經難以應對現代化攻擊的隱蔽性和規模化特徵。深度學習技術被廣泛應用於網路安全領域，特別是在 DDoS 攻擊的偵測與防禦中。本研究預期採用 CNN-GRU（卷積神經網路-門控循環單元）模型，結合空間特徵提取與時間序列建模的優勢。[19]

3.3.1 CNN-GRU 模型架構

CNN-GRU 模型的設計結合了卷積神經網路（CNN）與門控循環單元（GRU）的特性，具體模型用途參考表四內容[19]。

表四、CNN-GRU 模型架構功能[19]

單元	功能
CNN	用於提取網路流量的空間特徵
GRU	用於處理時間序列數據，可學習網路流量在時間上的演變特徵
全連接層與分類	通過 CNN 和 GRU 提取的特徵，最終輸入全連接層進行特徵融合，以區分正常流量與攻擊流量。

Nandanwar 使用深度學習 CNN-GRU 架構在 AttackNet 模型中實現了 99.7% 以上的偵測準確率，單一一維的 CNN 的模型準確度是 84%，2 維的 CNN 模型準確度是 87%，單一 GRU 的準確度則是 93%[19]。

3.3.2 模型訓練與數據集

為了訓練 CNN-GRU 模型，本研究預期採用公開的 CIC-IDS2017 和 CIC-IDS2019 數據集，這些數據集提供了豐富的網路流量數據和多樣化的攻擊樣本，涵蓋了 DDoS、DoS、SQL 注入、PortScan 等多種攻擊類型。這些能為模型提供比較全面的訓練數據，也能協助模型在不同攻擊場景下的防禦表現[16]。

根據公開數據集的特性，預期 CNN-GRU 模型能夠有效辨識大部分 DDoS 攻擊流量，並且在低誤報率和高準確率的基礎上，實現對未知攻擊類型的初步適應。這些模型輸出結果將進一步與 SIEM 系統整合，用於實時監控與通報。

3.3.3 偵測工具

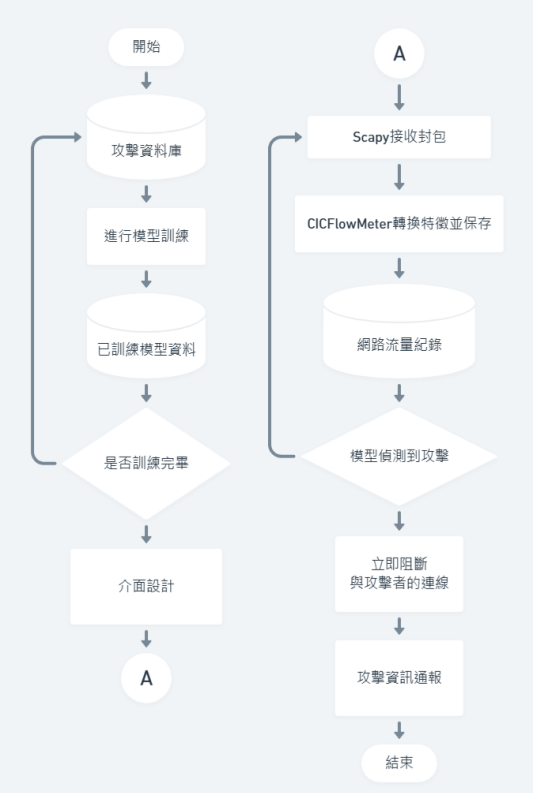
為了與 CNN-GRU 模型的輸入需求相匹配，本研究計劃預期使用 CICFlowMeter 工具，即時將原始網路封包數據轉換為流量特徵數據。CIC-IDS-2017 和 CIC-IDS-2019 數據集均使用該工具進行特徵提取，其特徵數據包括流量大小、平均封包間隔時間、源/目的 IP 地址等多達 80 多種的流量特徵。[5]

CICFlowMeter 的核心功能是將 PCAP 格式的封包解析為可用於深度學習模型的流量特徵數據。它能從封包的內容中提取 83 項特徵，包括協議類型、流量統計訊息、通訊方向等，這些特徵能夠表現網路行為。在數據轉換後，這些特徵數據將被用於 CNN-GRU 模型的訓練和推斷，從而實現對網路異常流量的檢測與辨識。[5]

我希望將本次專題實際應用設置在防火牆之後、核心交換機之前的位置，就此防火牆已經進行初步的封包過濾，能減輕系統的負擔，在該位置上可以檢查即將進入內部網路的流量，該位置也便於系統與現有的 SIEM 基礎設施整合，因為許多企業的日誌收集和安全監控系統也是部署在類似位置。

(四) 研究方法及步驟

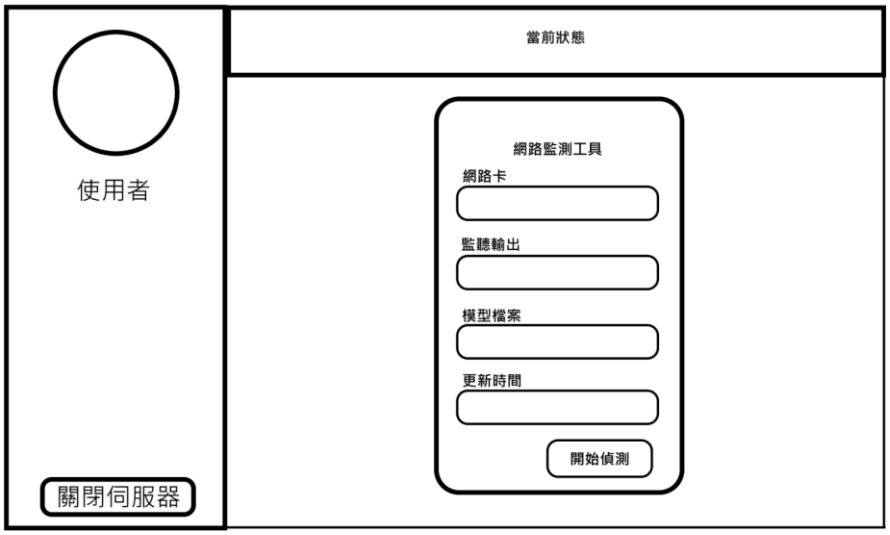
圖二是研究的流程圖，大概的描述研究的步驟流程。



圖二、研究方法及步驟流程圖

以下是研究的詳細步驟

1. 取得歷史攻擊資料：先取得攻擊的資料包，使用 CIC-IDS-2017、CIC-IDS-2019 及其他相關資料集進行分類。
2. 進行深度訓練：使用 CNN 來提取網路攻擊的特徵，並且利用 GRU 協助偵測網路前後的異常流量。透過使用 CNN-GRU 模型進行深度學習，訓練完成後將模型導出並保存，用作 DDoS 偵測的 AI 資料集。
3. 介面設計：使用 Django 框架來設計前端介面，圖三使用 HTML、CSS 及 JavaScript 來創建模板和頁面，並結合 Django 的視圖與模板系統來實現功能。



圖三、預計設定模板樣式

4. 使用 Scapy 網路監聽：將 Scapy 集成到 Django 應用中，捕捉網路封包並提取流量、來源 IP、目的 IP 等資訊。使用多執行緒來加速數據處理。
5. 使用 CICFlowMeter 提取網路監聽資料，並將網路封包轉成與 CIC-IDS-2017、CIC-IDS-2019 相同擷取特徵
6. 將網路即時資料、偵測資料自動保存至 SQL 資料庫，增加儲存效率；若偵測到 DDoS 攻擊時，將立即中斷與攻擊 IP 的連線。
7. 進行軟體測試，嘗試各種的 DoS 攻擊的情況，檢查是否能偵測到攻擊，如 DoS Slowloris、DoS Hulk 等等攻擊進行測試，確保系統的穩定性以及安全性。
8. 持續尋找更多網路攻擊工具進行模型訓練，攻擊的資料進行保存，並進行模型訓練，持續優化模型的準確度，確保能使模型有最高的實際效益。
9. 完全完善通報功能，遇到攻擊時，將自動通知使用者應如何應對網路攻擊，並且可以自動寫出通報資訊，協助完成資訊安全通報，減少工作流程。

(五) 預期結果

本研究的最終目標是開發一套具備 AI 自動化功能的 DDoS 偵測系統，實現快速且準確的攻擊流量辨識與通報，並整合多項功能以提高實用性與靈活性。

本研究主要預期新增以下幾點功能

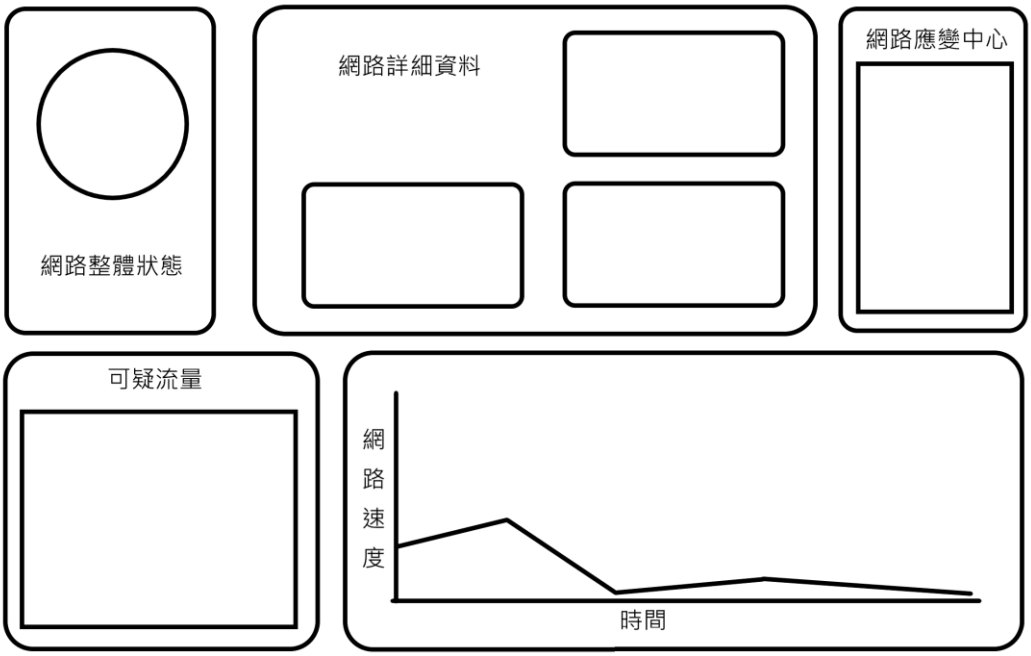
1. AI 自動化 DDoS 偵測與通報
2. 網路白名單與黑名單管理
3. 支援多網路卡偵測
4. AI 訓練與自訂訓練

本計畫預期能實現自動化的 DDoS 攻擊流量偵測，並且進行通報，例如高精度的偵測，藉由 CNN-GRU 深度學習模型對攻擊流量進行分析，預期達到 90%以上的準確度，同時降低誤報率至 5%以下，目前已有初步模型訓練測試，主要針對於 DoS Hulk、DoS slowloris 等進行測試，經過部分的 CIC-IDS-2017 的資料集以及部分透過收集攻擊流量，初步的攻擊辨識準確度(Accuracy)高達 80%，主要在遇到正常流量時會導致較多的誤報，預期能在未來的研究中降低誤報率。

在網路白名單以及網路黑名單管理方面，白名單管理將僅只准許預先授權的 IP 進行連線，其他流量自動阻斷，同時保留 AI 偵測，持續監控授權 IP 的流量，防止攻擊者通過 VPN、代理、偽造 IP 等方式攻破白名單系統。黑名單系統則在 IP 連線之前會先檢查是否在禁止連線名單中，即時阻斷黑名單連線，通過先前的 AI 偵測網路異常，自動將異常網路優先放置黑名單中，以防止後續對於偵測效能的浪費，藉此增進偵測速度。

除了 AI 自動偵測工具以外，本計畫也預期支援多網路卡偵測功能，預期讓使用者能夠在系統介面中選擇單一或多個網卡進行監控，使網路監控更加靈活且易於控制。另外預期系統可根據不同需求對網路數據進行保存與分類；本計畫也預期能增加自訂 AI 訓練功能，可以透過資安相關人員自行手動新增資料訓練 AI，增強在某個特定攻擊的資安防護，使得製作出來的成品更有彈性化，這樣的方式可以避免現有的模型資訊過於老舊，會在訓練資料的旁邊進行提示，說明如何正確的添加資料，避免格式不正確等問題產生；透過額外新增的新型訓練也可以防範未然，將沒有偵測到的內容直接新增到額外的模型數據庫內部，從而實現更高的穩定性；AI 訓練功能成型後，也會提供預設內容，在訓練模型發生異常時，提供恢復原廠的功能，或是導出曾經訓練過的模型進行備份，之後即可將自行訓練過的模型放到其他裝置上，全程都採用視覺化界面，提供訓練模型的方式，使得這款軟體變得更加實用以及可自訂性。

如圖四，本計畫預期將資料整合到網頁上，這樣可以使得使用者更容易辨識內容，並且可以更直觀的知道 IP、詳細資料，通過即時的通報系統知道如何進行應對，從而增加工作效率，通過放到網頁上，可以使得多平台裝置支援，透過遠端連線的開放，可以使得平板電腦、手機、桌上型電腦等裝置支援控制。



圖四、整體網頁偵測布局樣式

(六) 需要指導教授指導內容

需要教授指部分內容如 CNN-GRU 深度訓練的方法等問題，如卷積神經網路的訓練建議應用在哪一個部分，如何去使用尋找特徵狀態等，在循環神經網路，要如何注意時間軸，在訓練過程中避免時序問題導致偵測失效，還有更多的是資訊安全相關問題。

增加資料包時，應注意的各項項目等問題，使用何種模型訓練演算法等，對於訓練項目的精進調整，確保在一般使用的情況下是否符合預期準確度。

在測試軟體時，也會需要詢問教授如何去模擬 DDoS 的情境，在實際情況下如何呈現與當時相同的攻擊，在實驗時，確保軟體的可靠性，能在攻擊期間將異常網路擋下甚至是中斷連線。

(七)參考文獻

[1] 周峻佑（2023 年 11 月 10 日）。ChatGPT 與相關 API 服務發生間歇性中斷事故，OpenAI 坦承是遭遇大規模 DDoS 攻擊所致。 iThome。取自 https://www.ithome.com.tw/news/159733

[2] Cloudflare （n.d.）。什麼是 DDoS 攻擊？。Cloudflare。檢索日期：2025 年 1 月 31 日。取自 https://www.cloudflare.com/zh-tw/learning/ddos/what-is-a-ddos-attack/

[3] 維基百科 （2025 年 1 月 7 日）。阻斷服務攻擊。維基百科。取自 https://zh.wikipedia.org/wiki/阻斷服務攻擊

[4] GAIA Information Technology（2024 年 1 月 15 日）。分散式阻斷服務攻擊(DDoS)是什麼？遇到攻擊有哪些解決方法？ GAIA。取自 https://www.gaia.net/tc/news_detail/2/52/ddos-ddos

[5] datthinh1801（2022）。cicflowmeter。GitHub。取自 https://github.com/datthinh1801/cicflowmeter

[6] 數位通國際（2024 年 12 月 1 日）。DDoS 攻擊是什麼？如何進行 DDoS 防禦防護？攻擊原理手法詳解。eASPNet。取自 https://www.easpnet.com/blog/ddos-service/

[7] Fortinet (n.d.)。 什麼是 ICMP（互聯網控制消息協議）？ Fortinet。檢索日期：2025 年 1 月 31 日，取自 https://www.fortinet.com/tw/resources/cyberglossary/internet-control-message-protocol-icmp

[8] ExplainThis (2023 年 11 月 22 日)。什麼是 DDoS 攻擊？如何防禦？ ExplainThis。取自 https://www.explainthis.io/zh-hant/swe/what-is-ddos?utm_source=chatgpt.com

[9] Yoachimik, O., & Pacheco, J. (2025 年 1 月 21 日)。Record-breaking 5.6 Tbps DDoS attack and global DDoS trends for 2024 Q4。Cloudflare。取自 https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/

[10] 王智仁（2024 年 10 月 24 日）。NETSCOUT 2024 威脅情報：DDoS 攻擊急劇上升，威脅全球關鍵基礎設施。網管人。取自 https://www.netadmin.com.tw/netadmin/zh-tw/snapshot/6C47A2E526D74B148CBAB9A0C4914D46

[11] 編輯部（2024 年 10 月 29 日）。NETSCOUT：DDoS 攻擊急劇上升，威脅全球關鍵基礎設施。Information Security 資安人科技網。取自 https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=11342

[12] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759. https://doi.org/10.3390/s21144759

[13] Salam, A., Ullah, F., Amin, F., & Abrar, M. (2023). Deep Learning Techniques for Web-Based Attack Detection in Industry 5.0: A Novel Approach. MDPI. https://doi.org/10.3390/technologies11040107

[14] 林詠章 & 馬毅凱 （2023 年）。基於 API 解析及運用深度學習的工業自動化及控制系統惡意軟體偵測機制。台灣儀器科技研究中心。取自 https://www.tiri.narl.org.tw/Publication/InstTdy_Full/12649?PubId=234

[15] Palo Alto Networks. (n.d.). What is security information and event management (SIEM) software?. Retrieved February 3, 2025, from https://www.paloaltonetworks.com/cyberpedia/what-is-siem-software

[16] Canadian Institute for Cybersecurity. (n.d.). Intrusion detection evaluation dataset (CIC-IDS2017). University of New Brunswick. Retrieved February 5, 2025, from https://www.unb.ca/cic/datasets/ids-2017.html

[17] MetaAge （2023 年 4 月 12 日）。DDoS 攻擊定義 & 意思，與 DoS 有什麼不同？防禦方法 / 攻擊案例解析。取自 https://www.metaage.com.tw/news/technology/504

[18]羅正漢 （2020 年 1 月 9 日）。2020 十大資安趨勢 3：OT 安全。iThome。取自 https://www.ithome.com.tw/news/135175

[19] Nandanwar, H., & Katarya, R. (2024). Deep learning enabled intrusion detection system for Industrial IOT environment. *Expert Systems with Applications*, *249*(C), 123808. from https://doi.org/10.1016/j.eswa.2024.123808

[20] Microsoft. (n.d.). What is SIEM? Microsoft Security. Retrieved February 10, 2025, from https://www.microsoft.com/en-US/security/business/security-101/what-is-siem

[21]Cloudflare.(n.d.). What is SIEM? Retrieved February 10, 2025, from https://www.cloudflare.com/learning/security/what-is-siem/

表 C802