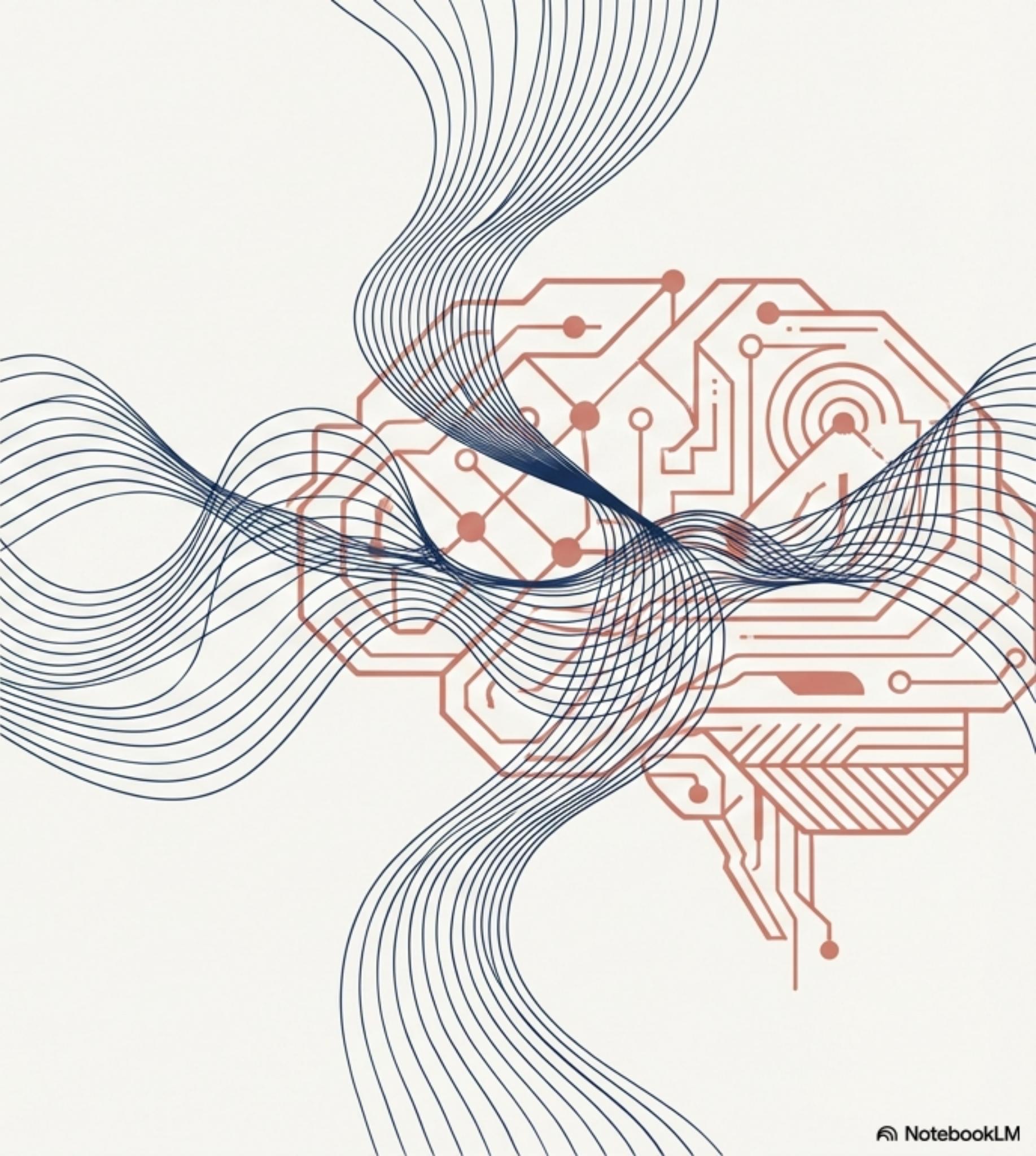


# 智慧反擊：從 DDoS 攻防演進到深度學習 防禦策略最佳化

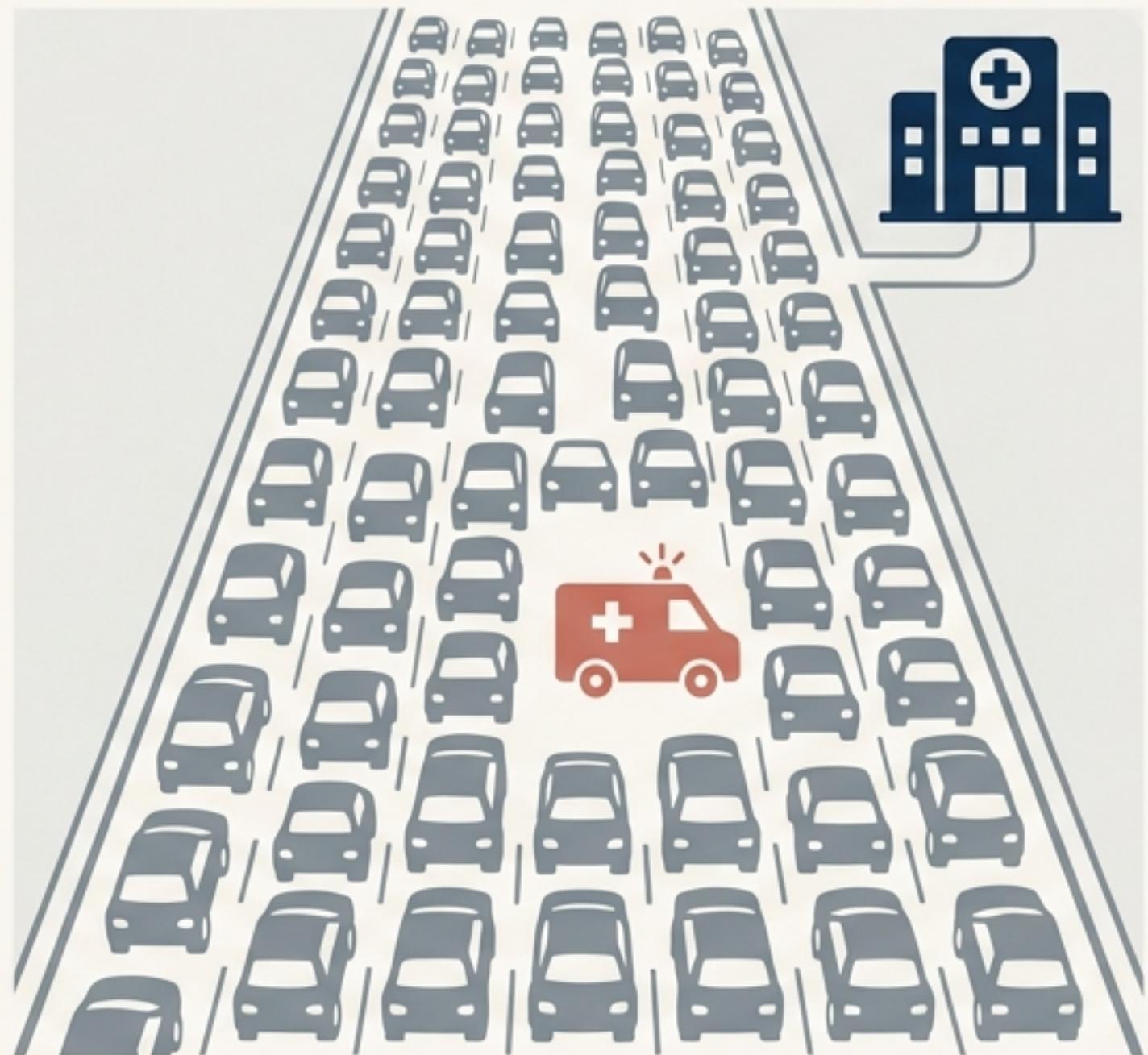
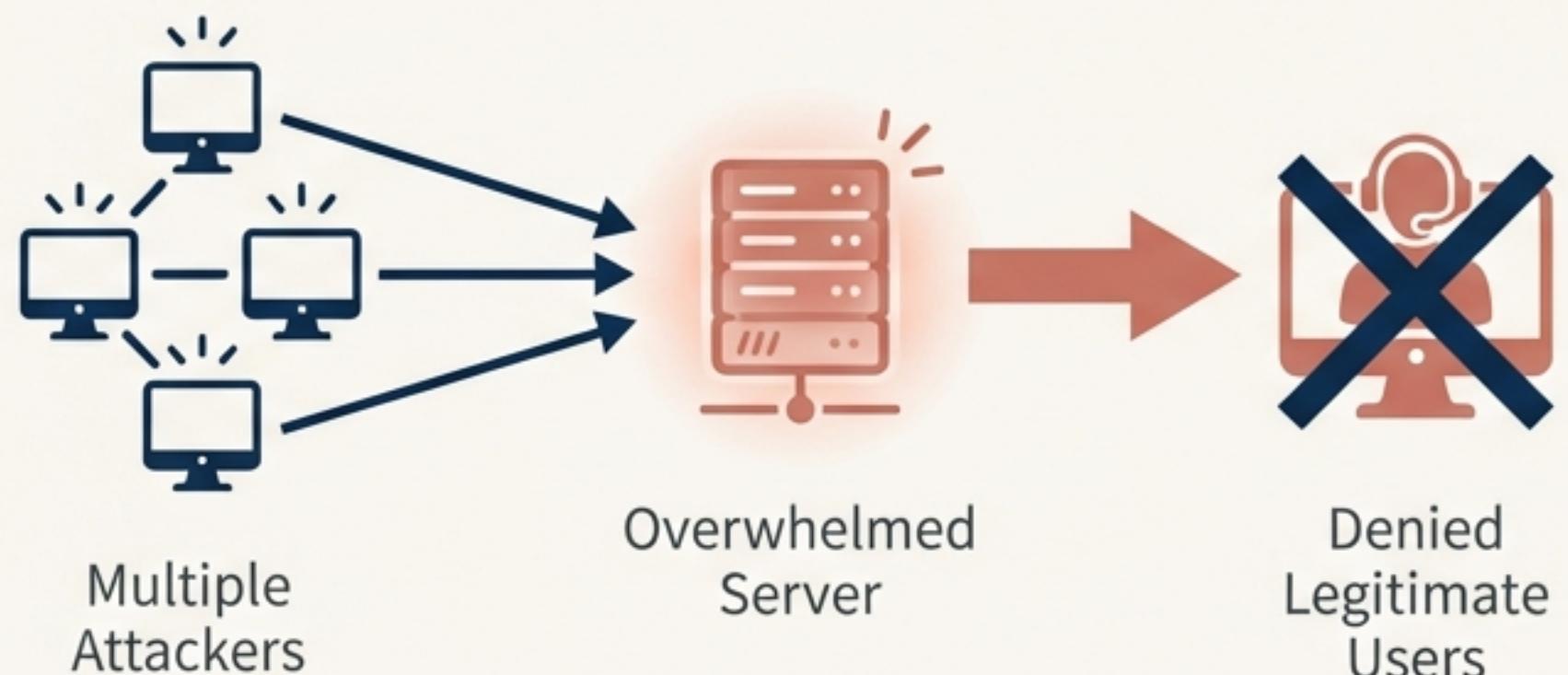
碩士論文研究計畫與進度報告



# DDoS 攻擊：癱瘓服務的數位洪水

定義：分散式阻斷服務攻擊 (Distributed Denial-of-Service)。

核心目的：透過海量請求癱瘓目標伺服器或網路資源，使其無法向合法用戶提供服務。



# 攻擊的演進：從「量變」到「質變」

量 (Quantity)



Title: Layer 3/4 攻擊 (網路/傳輸層)

Example: SYN Flood

Keyword: 頻寬消耗

質 (Quality)



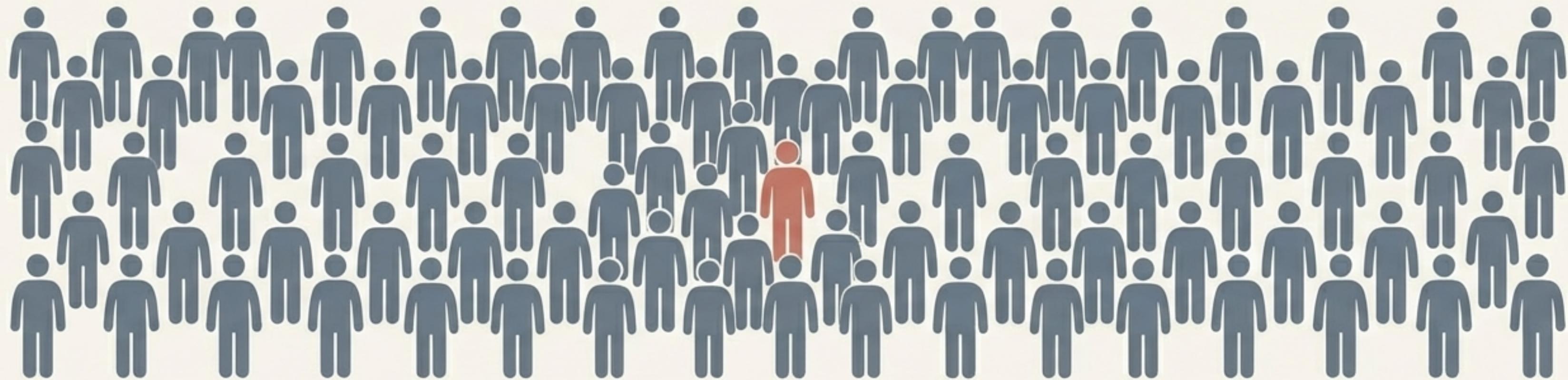
Title: Layer 7 & Low Rate 攻擊 (應用層)

Example: HTTP Flood, Slowloris

Keyword: 資源/邏輯消耗

攻擊者不再只是在城門外衝撞，而是偽裝成合法用戶，從內部消耗系統。

# 為何新型態攻擊如此棘手？



## 核心難點：難以與合法流量區分

它們模彷正常用戶行為，以低頻率、長時間的方式發動，利用協議漏洞或伺服器資源超時機制。

- Slowloris : 佔用所有伺服器連線數
- RUDY : 發送少量 Headers，緩慢傳輸 Payload

如何在不影響所有正常用戶的情況下，找出隱藏的威脅？

# 當傳統規則失效，我們需要能學習與適應的智慧防禦

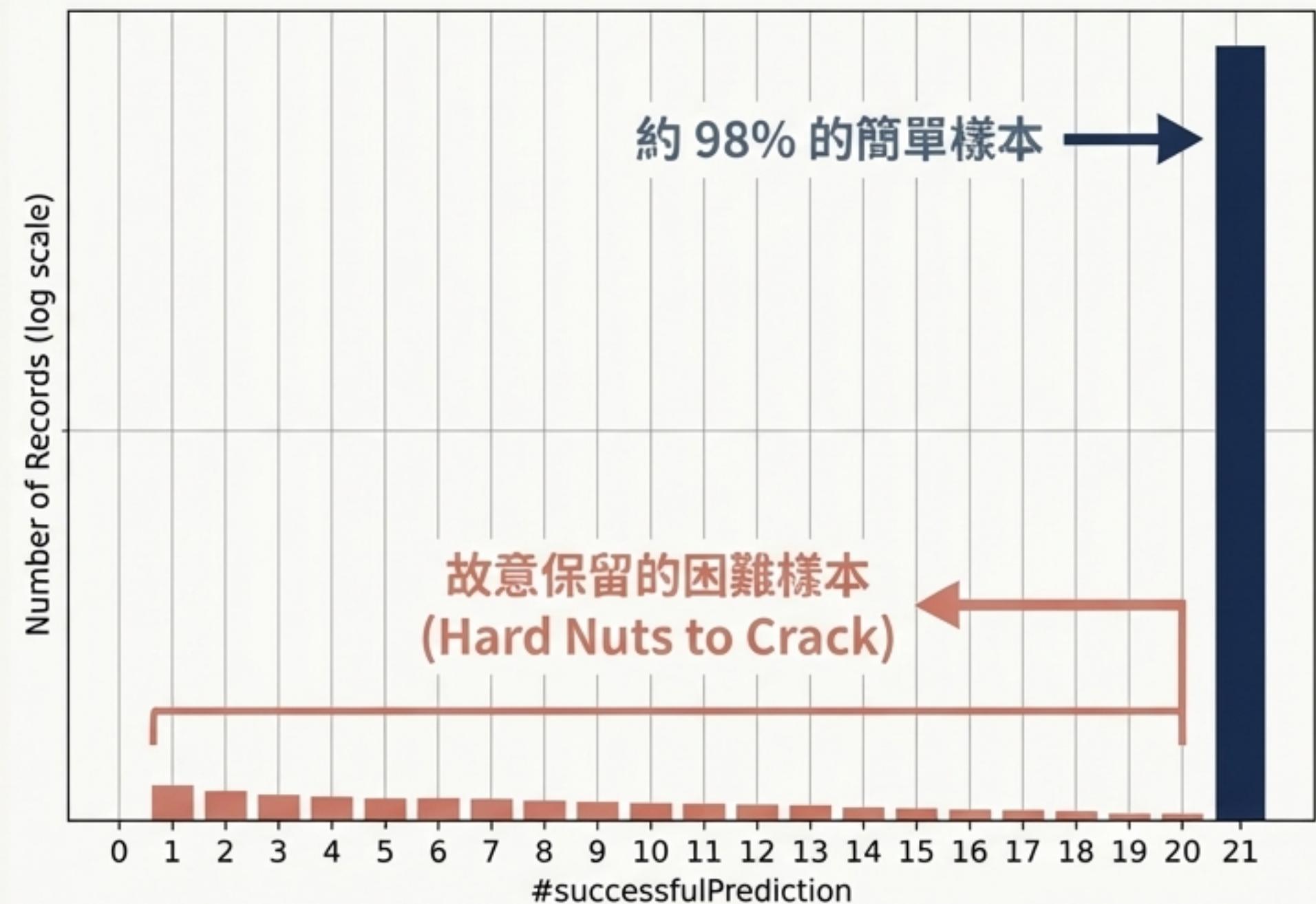


Thesis Title : 基於深度學習之網路異常流量偵測與多目標策略最佳化

Core Research Objective : 本研究旨在開發並評估一個深度學習框架，不僅能偵測複雜的異常行為，更能在真實世界的維運限制下，對防禦策略進行系統性最佳化。

# 我們的試煉場：專為挑戰 AI 模型設計的數據集 (NSL-KDD)

- 解決了舊 KDD99 資料集的缺陷：移除冗餘樣本，改善類別不平衡問題。
- 關鍵創新：引入 "Difficulty Level"，確保模型在最模糊、最難分類的樣本上進行訓練，而不僅僅是簡單的樣本。



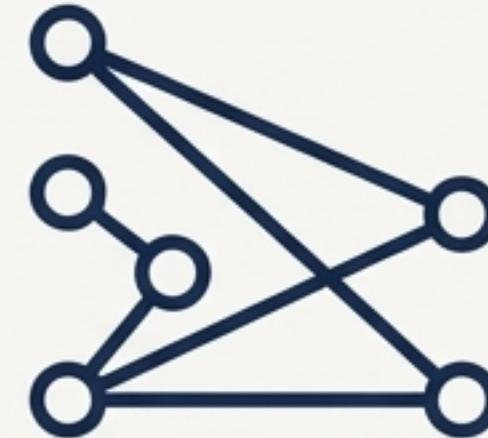
# 我們的武器庫：從序列到關係，全方位解析流量模式



**LSTM（長短期記憶網路）**

**歷史學家**

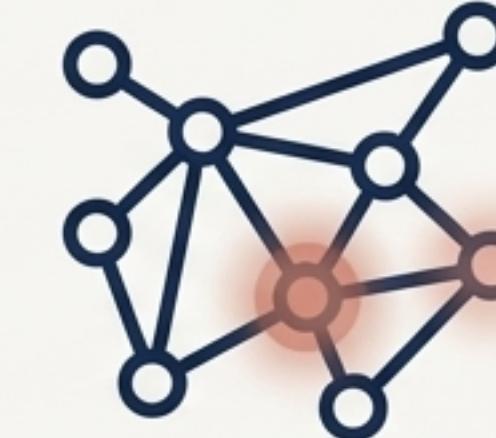
擅長理解事件的時序與時間依賴性。



**Transformer**

**策略家**

能看見複雜數據流中的長距離關聯性。



**GNN（圖神經網路）**

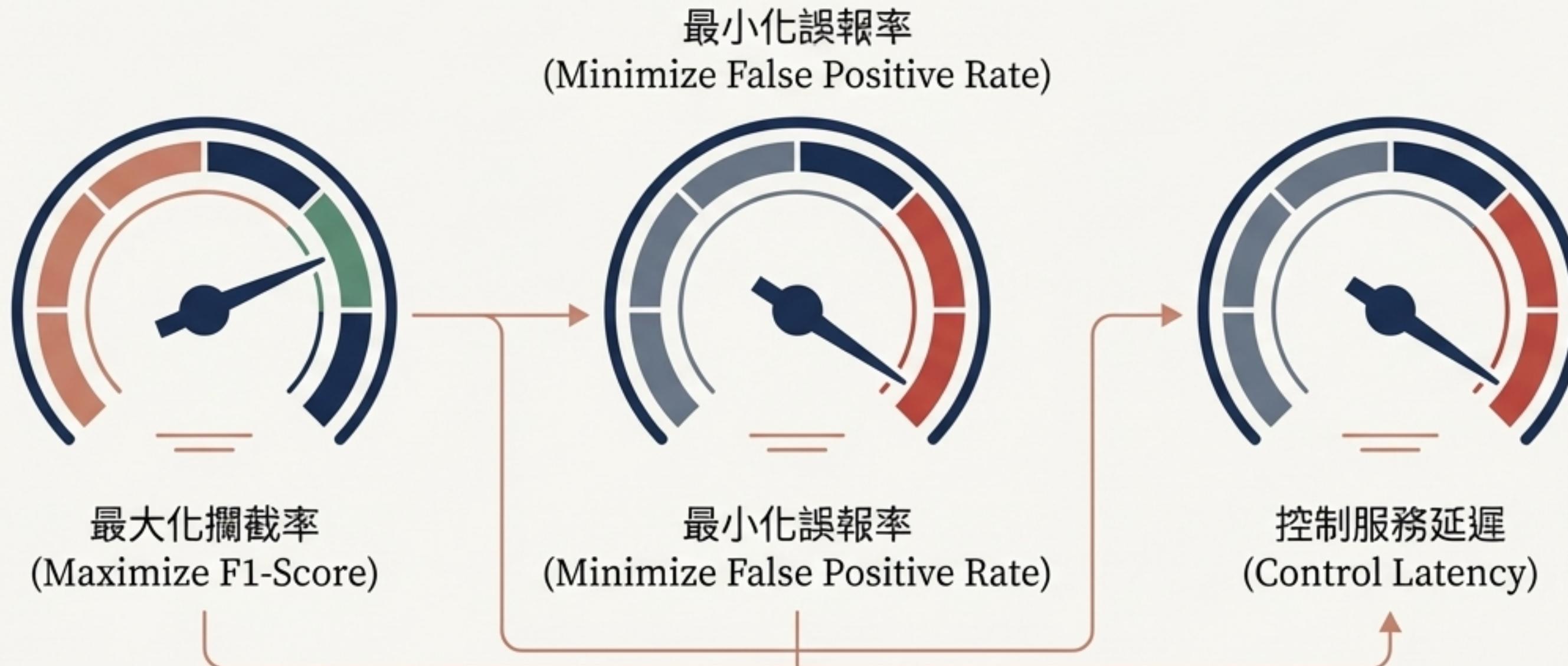
**社群網路分析師**

透過繪製實體間的關係圖（IP、用戶），揭露協同攻擊與異常連結。

我們不只使用一種工具，而是結合不同模型的視角，從「序列」和「關係」兩個維度來定義異常。

# 防禦的藝術：在多重目標間尋找最佳平衡點

現實世界的防禦並非只有「攔截」單一目標，而是一場艱難的權衡。



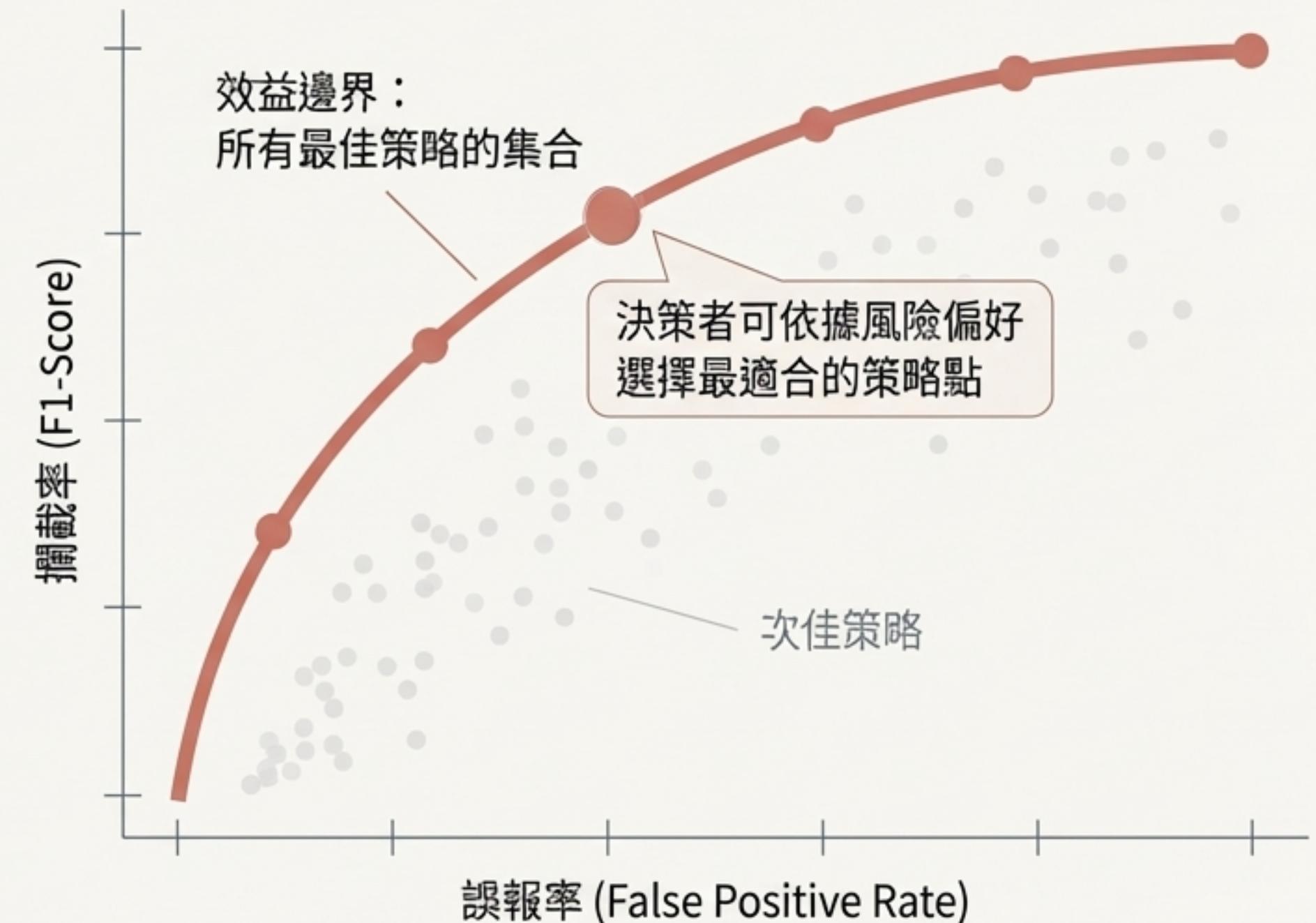
# 我們的決策引擎：以貝氏最佳化繪製效益邊界

The Method:

我們使用**貝葉斯最佳化 (Bayesian Optimization)**，一種智慧搜尋演算法，它能在不測試每種可能性的情況下，高效地找到最佳參數組合（如偵測閾值）。

The Outcome:

研究成果將以**帕雷托前緣 (Pareto Front)** 圖呈現。



# 研究範疇：專注核心，定義邊界

## 研究範疇內 (In Scope)



- 模型實作與比較 (LSTM, Transformer, GNN)
- 使用公開資料集 (NSL-KDD, CIC-IDS2017)
- 應用貝葉斯最佳化進行策略權衡分析
- 評估指標 (AUROC, F1-Score, Latency, FPR)

## 研究範疇外 (Out of Scope)



- 大規模資料平台建構 (Spark, Kafka)
- 系統整合與正式環境部署
- 後量子密碼學 (PQC) 的工程實作
- 開發全新的深度學習模型

# 我們要回答的核心問題

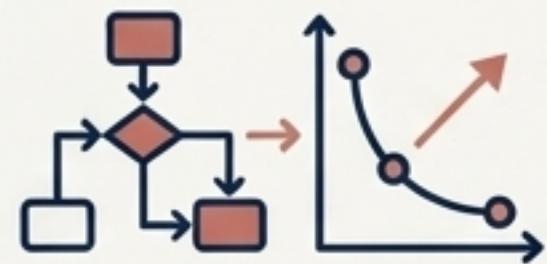
1. **模型效能比較**：在公開資料集上，LSTM、Transformer 與 GNN 等不同深度學習架構，何者在網路異常偵測任務上表現最佳？
2. **策略權衡最佳化**：如何透過貝葉斯最佳化，在最大化攔截率、最小化誤報率及控制延遲等多重維運目標間，找到系統性的最佳平衡策略？
3. **前瞻影響分析**：未來導入後量子密碼學 (PQC) 可能增加的延遲，將如何影響我們所找到的最佳防禦策略邊界？

# 預期貢獻：從學術基準到實務框架



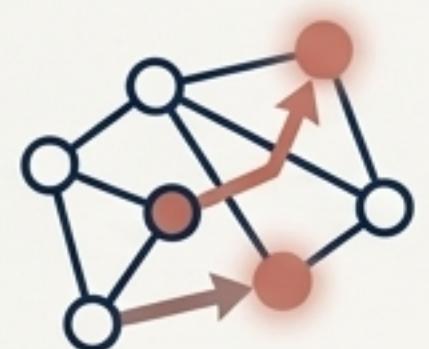
## 嚴謹的模型效能比較基準

針對三種主流深度學習模型，在公開資料集上提供一份系統性的量化效能比較，供學術界與業界參考。



## 系統性的決策最佳化框架

展示如何應用貝葉斯最佳化，將複雜的資安防禦權衡問題，轉化為一個可視化、數據驅動的決策框架 (Pareto Front)。



## GNN 於資安應用的實證探索

為圖神經網路這個前沿方法在網路安全領域的應用，貢獻新的實證數據與見解。

# 研究時程規劃

|                     | M1-M3   | M4-M6   | M7-M9   | M10-M12   |
|---------------------|---|---|---|---|
| 第一階段：文獻探討與研究計畫確立    |  |   |   |   |
| 第二階段：資料集搜集與前處理      |   |  |   |   |
| 第三階段：核心模型實作與策略最佳化實驗 |   |   |  |   |
| 第四階段：論文撰寫、修正與定稿     |   |   |   |  |

# 展望未來：從後量子密碼到跨領域應用

## Forward-Looking Cybersecurity

**PQC 影響<sup>\*\*</sup>:** 我們的延遲與成本分析框架，能為未來網路協定遷移至後量子密碼學 (PQC) 時的決策提供理論基礎。

## Broader Impact & Cross-Domain Value

本研究的核心是「高維數據中的異常偵測框架」。此框架的價值不僅限於資安，更能直接應用於：



**輔助科技**：偵測病患的異常生理數據或行為模式。



**半導體/光電製程**：探勘生產數據，預警設備故障或良率異常。

這項研究不僅解決了資安問題，更打造了一個可在多個科學與工程領域應用的分析工具。

# 感謝聆聽 & 問題與討論

姓名: [Presenter's Name]

Email: [Presenter's Email]