2026 臺灣數創大賞決賽

(智慧+組)

智慧硬體資安檢測與風險平台

115634 隱私守門員

1 看不見的資缺口 零操作失誤，資訊仍可能外洩



正常使用電腦

員工沒做錯任何事，

資訊照樣外洩。

鍵盤聲學側錄



收錄打字聲，

就能還原輸入內容

系統資源側寫



系統資源數據，

推出你在瀏覽的網站



2 攻防一體：先看見風險，再親手驗證防禦

不只是警告，而是理解與驗證 —— 每項防禦皆附原理說明，可親手切換比較

漏洞檢測



檢測硬體

可能的旁通道風險

真實攻擊



還原輸入內容

辨識瀏覽網站

資安檢測與風險平台



隱私守門員

啟用防禦



一鍵切換

A / B / C 防禦方案

驗證成效



比較防禦前後

攻擊成效差異

3 雙軌真實攻示範

A 鍵盤聲學辨識：你在打什麼



聲學波形 → CNN 特徵擷取 → 模糊字典比對 → LLM 語意校正 → **75.27%** 語句還原 BLEU分數

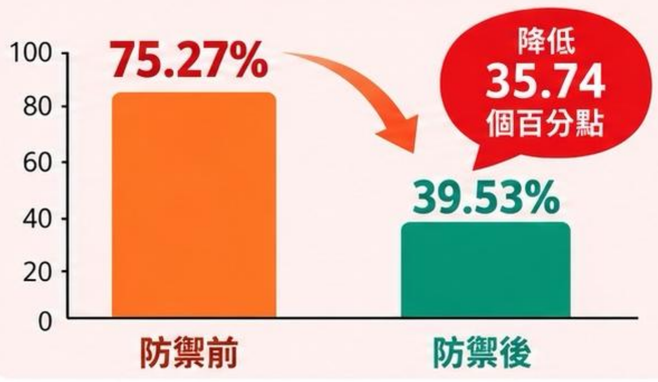
B 網站指紋識別：你在看什麼



系統資源數據 → 時序分支 → 頻域 FFT 分支 → 統計分支 → 融合 → **97.93%** 網站辨識準確率

4 防禦成效：用數據證明有效

句子完全正確率（防禦 A）



網站辨識準確率（防禦B）



三種防禦方案

A 打字聲遮蔽

注入誘餌按鍵聲，污染按鍵切割



B 資源掩護雜訊

非週期負載雜訊，避開 FFT 濾除



C 系統級防禦 App

防禦 A + 防禦 B +

偵測監測工具即時示警



AiCTSP 台灣臺中軟體園區發展產學訓聯盟 Academia-Industry Consortium of Taichung Software Park in Taiwan

TUNGHAI UNIVERSITY 1955

SYSTEX 精誠資訊

雄欣科技 IAMBITION TECHNOLOGY CO., LTD.

TCCA 台中市電腦商業同業公會

Digipark