國立成功大學 資訊工程學系
Department of Computer Science and Information Engineering

OTX威脅情資蒐集系統及其應用

指導教授:**張燕光教授**

學生: F74126149 林欣懋、F74127064 彭志光

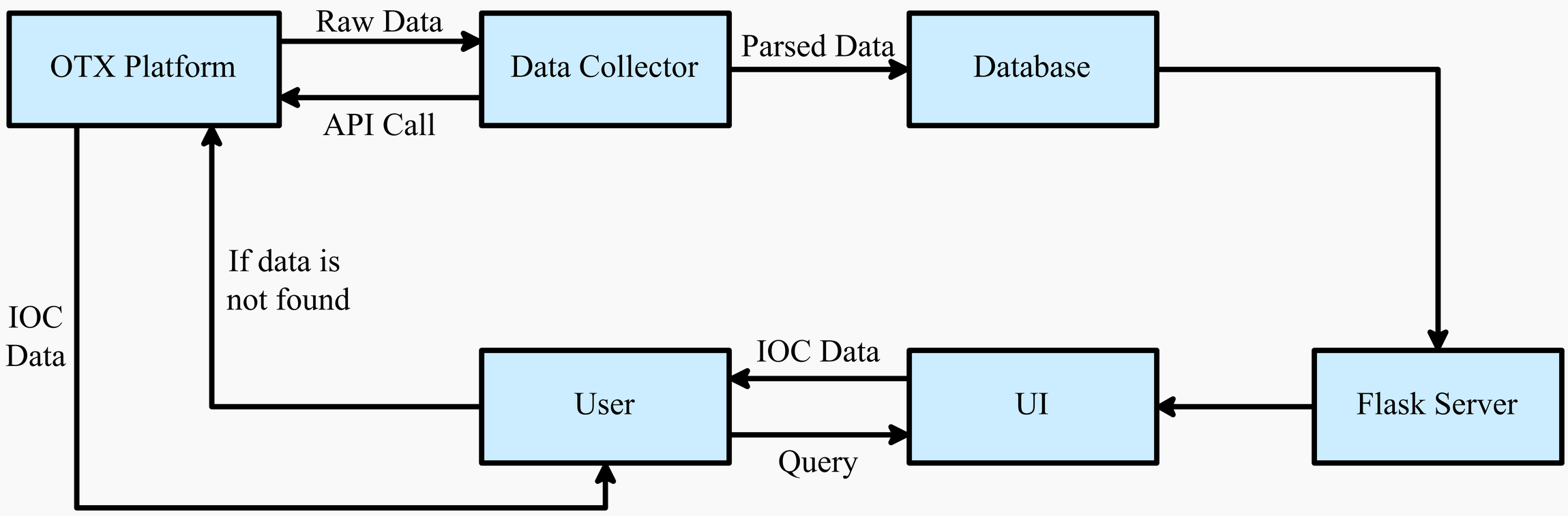
I. 研究動機及目的

隨著網路使用量日漸增長，資訊安全的重要性也逐漸提升。近年來，釣魚網站、惡意網址、惡意程式下載與網路攻擊事件頻繁發生，使用者在瀏覽網站或下載檔案時，可能在不知情的情況下遭受各種資安威脅。

為了降低使用者接觸惡意網站的風險，本專題決定建立一套「惡意網站／釣魚網站偵測系統」，基於 **OTX（Open Threat Exchange）**平台，自動蒐集威脅情資並建立 **IOC（Indicators of Compromise）**資料庫。

同時提供小型查詢視窗，讓使用者在瀏覽網站時能快速輸入 **IP、Domain** 或 **URL** 進行查詢，即時取得對應 **IOC** 的威脅資訊。

II. 系統架構圖



III. 實作技術與環境

- **Python** → 主要開發語言
- **OTX API** → 威脅情資來源
- **Requests** → **HTTP** 請求與 **JSON** 解析
- **SQLite** → 建立 **IOC** 資料庫
- **Flask** → 前端與查詢介面
- **Docker** → 容器化部署環境

IV. 結果

本專題成功建置一套達成前述目標的系統，能夠有效的蒐集威脅情資，並將其用於協助使用者抵禦潛在的網路安全風險。

V. 結論與未來展望

本次實作完成了 **IOC** 的搜尋、儲存與查詢等功能，後續可整合 **SOC、SIEM、Firewall** 或瀏覽器擴充功能，作為進一步的資安防護應用。

Demo 影片