

結合大語言模型的系統監控與自動化平台

AI Powered Monitoring and Automation Platform

指導教授：張瑞紘 專題成員：莊智皓

專題概要 Project Overview

現代企業與雲端環境的服務數量與複雜度持續攀升，傳統監控工具需安裝代理程式且仰賴人工經驗，難以即時應對多變的異常狀況。為此，本專題提出一個結合大語言模型的系統監控與自動化平台，旨在自動化地對各類服務進行即時監測，並利用 LLM 的推理與生成能力，針對異常事件提供具體的修復建議，甚至觸發預先定義的自動化動作，期望降低維運門檻，提升整體系統的安全性、穩定性與管理效率。

圖形化介面

透過拖曳與連接各個節點來定義流程
沒有程式門檻也可以輕鬆操作

LLM 分析與決策

借助 LLM 對各項指標進行分析
並且能夠推薦使用者適合的應對措施

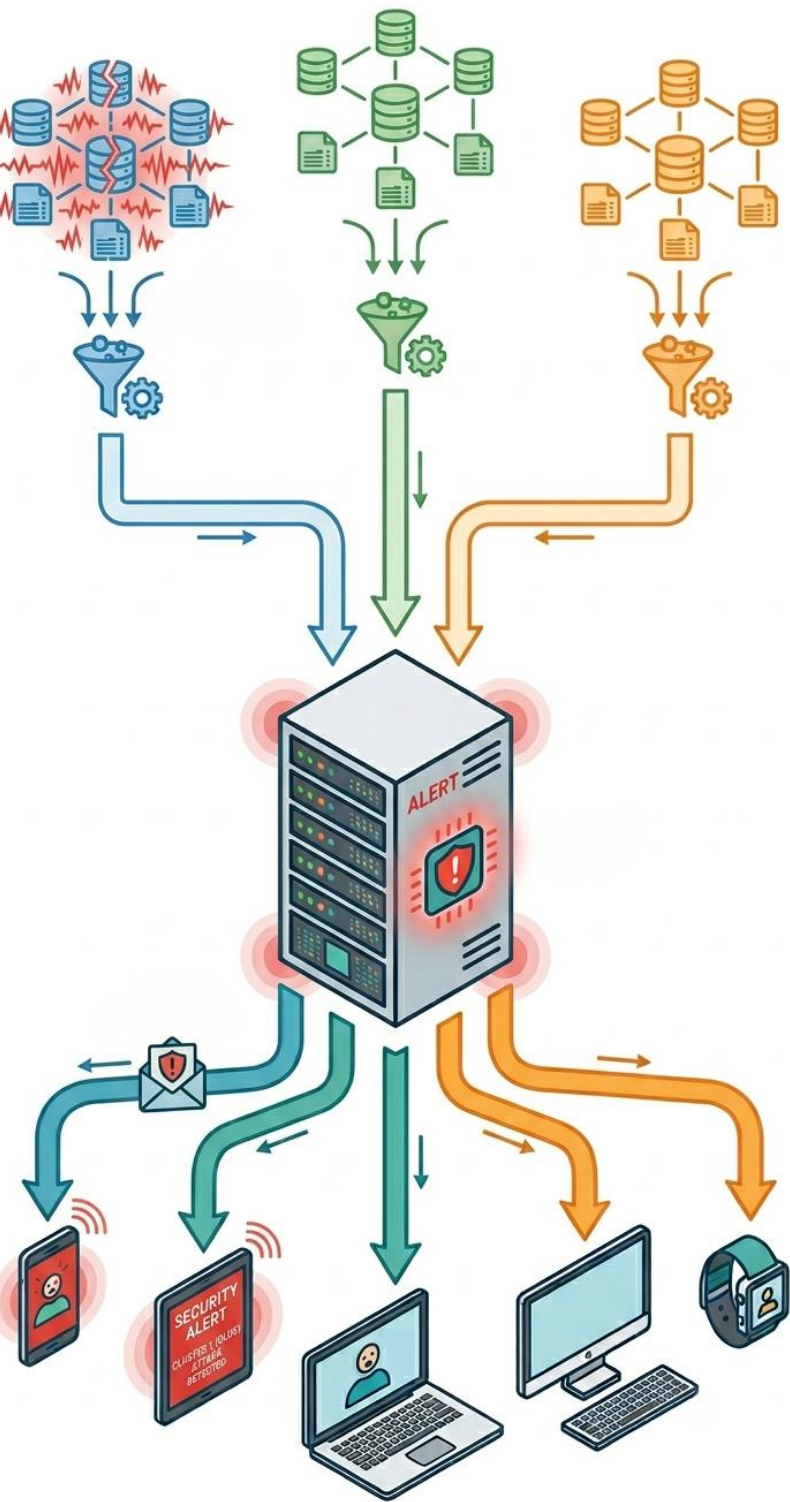
流程自動化

透過自訂的判斷流程
能夠即時針對異常行為進行動作

系統架構與技術 Architecture & Tech Stack

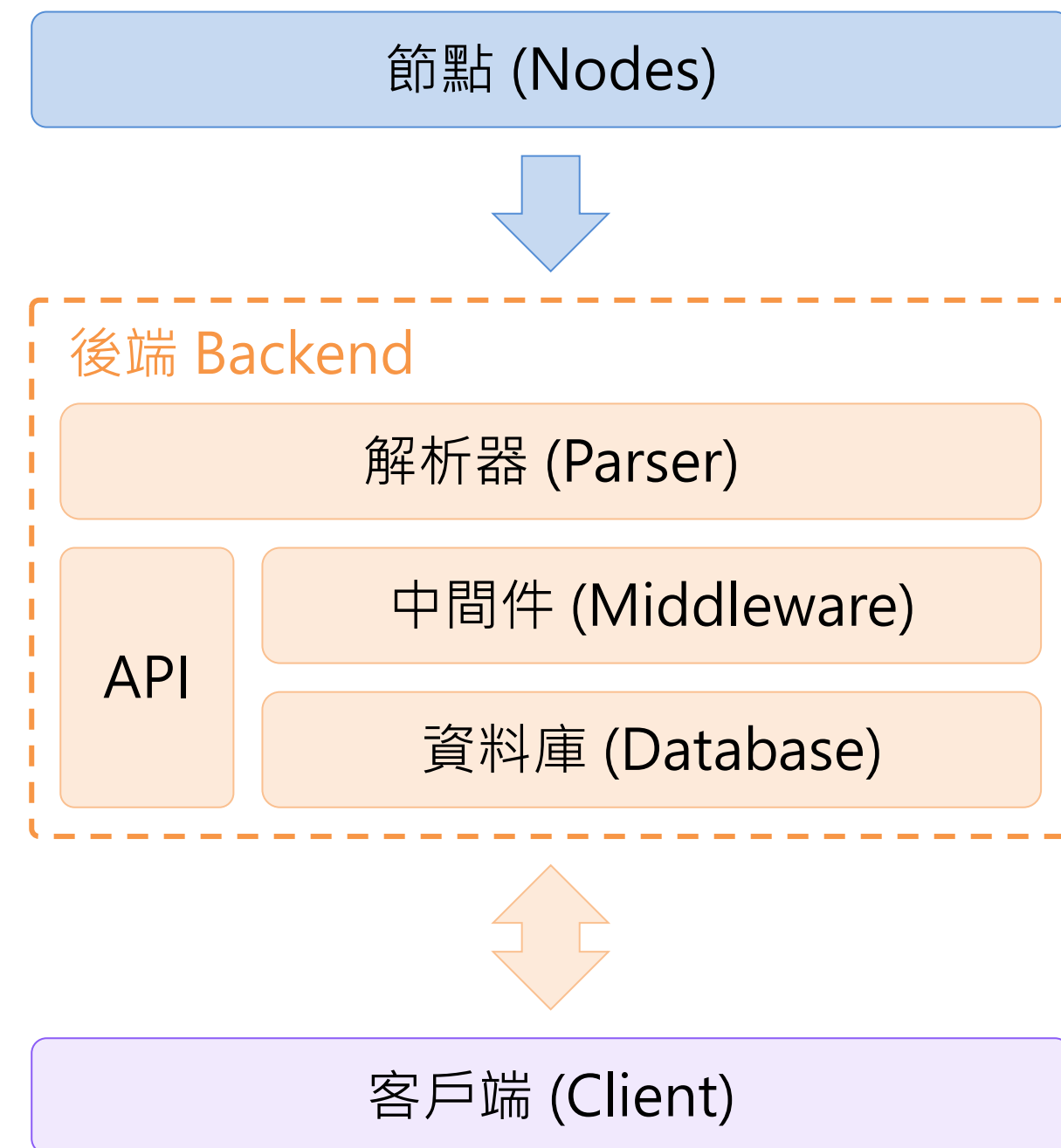
整體架構與技術

- 主要流程是先將各個節點上的資料先傳送至伺服器後，由伺服器進行解析與判斷，最後再透過網頁呈現給使用者。
- 資料蒐集程式使用 C 語言進行實作，並搭配 JWT 的簽章機制進行簡單驗證與防竄改。
- 後端使用 Python 的 FastAPI 框架，其支援非同步 (Async) 的特性能夠讓系統在此類 I/O 密集型的任務下仍可維持較高的效能。
- 資料儲存使用了 TimescaleDB 作為資料庫，並搭配 Hasura 來讓前端可以輕鬆地透過 GraphQL 對資料進行彈性的查詢。



核心功能與邏輯

- 這套系統除了最基礎的數據視覺化以及固定閾值發送通知的功能以外，還設計了一套能夠由結合大型語言模型的自動化系統。
- 依照使用者所設計的流程，當每次接收到資料時，系統會將輸入的資料進行分類、整理，如果符合特定條件時，就會將資料與各項資訊一起發送給 LLM 進行分析。
- 收到 LLM 的回覆之後，系統會根據分析的結果及程度向使用者發出通知。
- 除了單純的通知以外，也可以藉由預先定義函數，讓 LLM 了解能夠進行那些操作並生成對應的參數，並推薦使用者應該進行甚麼操作，而使用者只須要簡單的按下接受便能夠自動運行。

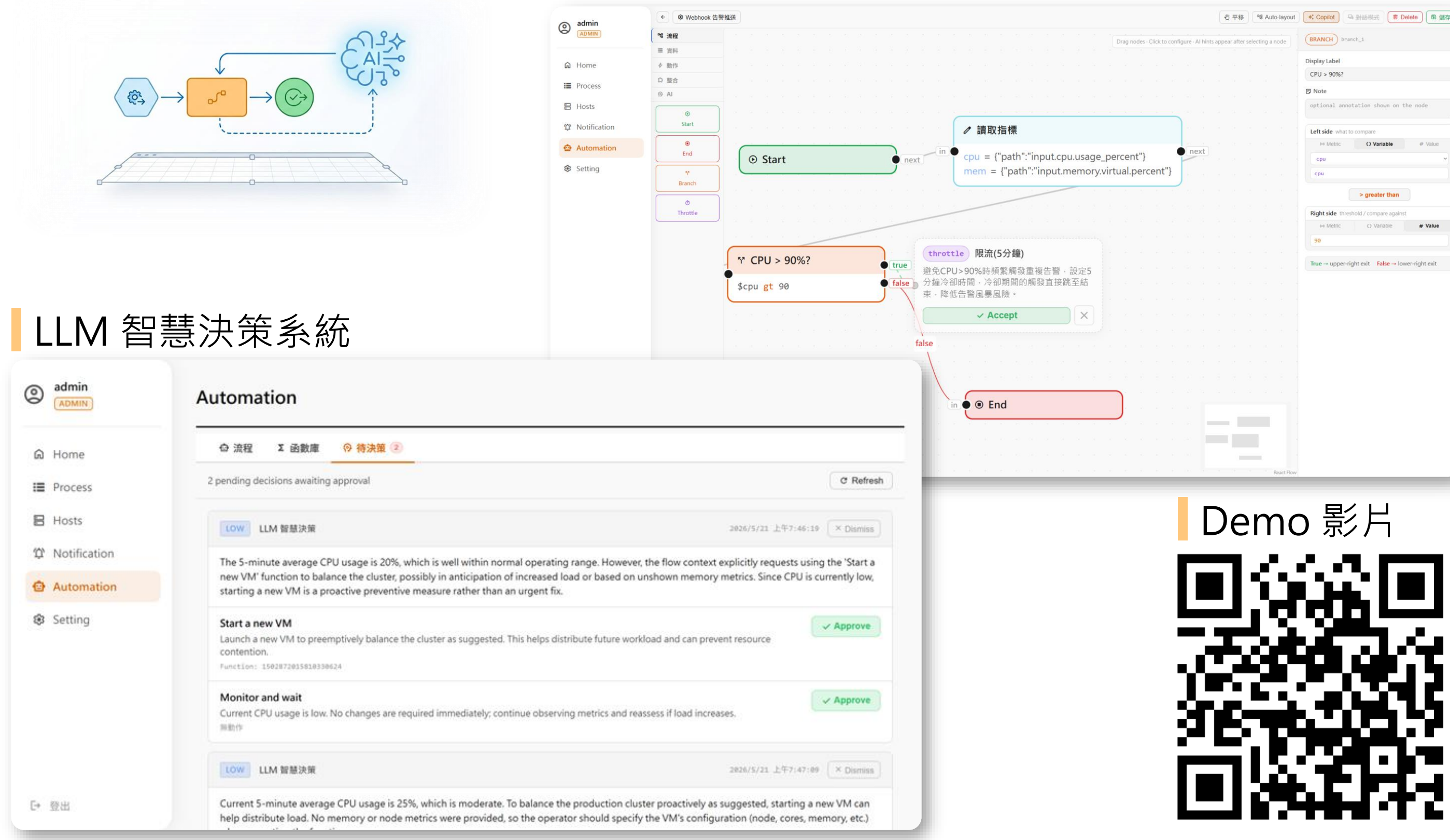


結論與未來展望 Conclusion | 成果展示 Results

本專題開發出一套結合大語言模型的系統監控與自動化平台，並且擺脫了傳統監控工具對特定作業系統與終端裝置的依賴，讓維運人員不受時間與地點限制即可掌握服務狀態。在資訊安全的應用上，本平台不僅止於效能監控，更能將大語言模型的推理能力與自動化流程延伸為主動式的資安防護。

未來，希望能夠繼續對此系統進行改進，期望能夠透過引入 RAG 使 LLM 不僅僅只根據當前的情況作出應對，更能結合過去的經驗與事件，提出更適當的處置與建議，甚至能夠透過各項資料提前發現威脅，進而讓使用者能夠有更多的時間進行應對與防堵。

圖形化的流程編輯介面



Demo 影片

