

**二、研究計畫中英文摘要：**請就本計畫要點作一概述，並依本計畫性質自訂關鍵詞。

(一) 計畫中文摘要。(五百字以內)

**總計畫：支援行動應用 APP 之惡意風險分析及使用者認證技術研發**

因雲端運算技術、智慧行動裝置的蓬勃發展及行動網路的普及，行動裝置與雲端運算結合的行動雲端應用，已成為熱門的發展方向之一。然而，行動雲端應用帶來龐大的商業機會也帶來許多資訊安全的議題，例如行動端裝置逐漸普及，個人的資料可能在不同的裝置上使用，這就衍生個人隱私與個人資料保護的資安議題。經研究團隊觀察發現除了植入惡意程式外，行動裝置身分認證機制失效(如肩窺帳號密碼)，也會有個人隱私或資料被竊取的疑慮。為此，本計畫案將研究內容分為三部分：首先，子計畫一將針對 APP 惡意程式提出一種創新的雲端隱匿聚合並評估 Android 可疑 APP 之惡意風險分析技術，不但利用雲端運算解決行動裝置資源不足的問題，還確保使用者是匿名傳送資料進行分析，不會經由分析工具造成個人隱私外洩。其次，子計畫二將針對操作姿態不同、特徵量化方式及多模式驗證架構等三方面改善過去研究成果，提供一個智慧型手機可適應多重操作姿勢且多模式的使用者識別技術，藉此提升身分認證技術的識別效能。最後，因子計畫一與二需要可即時性分析的雲端計算能力且須具備高可用性的運算環境，因此，子計畫三將建構雲端平台提供其他子計畫符合其需求的雲端運算架構且針對雲端服務高可靠度進行深入研究。

關鍵字：行動雲端；行動 APP 惡意程式分析；身分驗證；雲端高可用性

## 子計畫二：智慧型手機可適應多重操作姿勢的多模式使用者驗證機制研發

由於電子硬體技術與無線網路的迅速發展，促使智慧行動裝置快速發展，其產品涵蓋智慧型手機、平板電腦、智慧型手錶與手環等，其中，智慧型手機更成為存取資訊的重要裝置。然而，根據市調報告指出，有 60%-80% 的使用者會關閉裝置上的身分認證機制，而且文字或圖形密碼在開放環境中使用無法避免有心人士肩窺。因此，智慧型手機上的安全性需要提升與強化。根據本團隊最近幾年執行的研究計畫與學術發表的論文，已針對智慧型手機研發一系列的使用者識別機制；然而，我們發現可從三方面著手提升目前的識別效果：處理不同情境的操作姿態、使用統計特徵量化優於動態特徵量化方法、建構多模式識別優於單模式識別機制。因此，我們將根據不同的研究重點與技術內容，將研發過程分成二年，第一年將著重於使用智慧型手機的方位感測器與觸控螢幕收集操作行為資料，並以統計特徵量化為基礎，建構一個智慧型手機可適應多重操作姿勢的使用者識別機制。第二年，則以手錶內建的加速度計、陀螺儀與方位感測器收集行為資料，並套用我們過去在智慧型手機研究上的特徵量化與行為建模等技術，建構智慧型手錶上的使用者識別機制，最後，將手機與手錶兩者識別機制結合，建構一個智慧型手機多模式使用者識別機制。

關鍵字：智慧型手機；智慧型手錶；多重操作姿勢；行為特徵；多模式使用者驗證；