十一、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：支援行動裝置使用者與虛擬實驗平台之雲端技術研究

近年來，行動裝置已經成為普遍的雲端服務存取裝置之一，然而，行動裝置的可攜性與行動性帶來的不只是便利性，往往也帶來資料外洩等風險。因此，如何提升行動裝置使用者安全性是資訊安全中的一項重要議題。再者，利用雲端環境所提供的虛擬技術建立雲端虛擬實驗平台將是未來熱門議題，尤其是將網路安全攻防實驗部署於虛擬實驗平台，可以擁有較高的實驗安全性。除了虛擬實驗平台的設計與建構外，往往會因為實驗案例需要龐大的虛擬資源可能造成單一雲端資源不足，例如：DDoS 實驗，因此，如何運用多雲端基礎服務使得虛擬平台能夠順利運行也是本研究計畫研究的議題之一。為此，本研究計畫案將研究內容分為三大區塊，首先，子計畫一鎖定目前熱門的行動裝置平台，研究輔以現有識別機制的非侵入性連續使用者識別技術並利用子計畫二多雲端基礎服務確保服務品質。其次，由子計畫二設計與建構虛擬實驗平台並與子計畫三合作進行多雲端服務基礎服務研究。最後，子計畫三除了提供子計畫一與二基礎服務外，為了有效利用底層平台資源與確保雲端資料的安全性，將著重於負載平衡機制和虛擬機房保護與回復等研究議題。

關鍵字：雲端安全；使用者識別；虛擬實驗平台；多雲端基礎服務

子計畫一：雲客端—手持行動裝置使用者識別機制

由於資訊技術與網際網路的迅速成長，手持行動裝置(如：智慧型手機)不僅是用於通訊也可用於存取雲端服務。根據市調顯示，智慧型手機目前的主要應用是以電信通訊以外的服務為主流。而這些新應用也掀起新的安全議題—手持行動裝置與雲端服務現存安全機制是否足以維護存取雲端服務上隱私與敏感性資訊的安全？在手機防護方面，目前智慧型手機通常是以 PIN 碼、密碼為主，甚至是採用指紋或臉部等生物特徵的識別技術。然而，密碼與指紋這類型的安全性機制皆需要使用者執行一個特定的認證程序，屬於侵入式驗證的方式；市調也指出，有 60%-80%用戶會因侵入式認證不方便而選擇關閉該功能。在雲端存取安全防護部分，通常只採取密碼式安全認證，若以行動裝置進行存取，便有肩窺的安全問題。在安全性不足的情況下，採用手持行動裝置存取雲端服務恐成為雲端平台的安全罩門。因此，加入非侵入式的使用者識別機制是有其必要性。根據研究團隊的觀察，除了發現使用者會採用獨特習慣方式來持握與操作其手持行動裝置外，亦發現手持行動裝置內建感應器可擷取這些行為特徵。因此，本團隊提出一套適用於手持行動裝置的非侵入式使用者識別機制，雲端服務平台可以藉由此項機制防禦透過手持行動裝置的非法存取。

關鍵字：雲端安全；手持式行動裝置；智慧型手機；非侵入式認證機制