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。

計畫中文關鍵詞	智慧型裝置;智慧型手機;資訊安全;行為特徵;使用者驗證;使用者偽造攻擊;特徵權重排名
計畫英文關鍵詞	Smart device; Smartphone; Information security; Behavioral patterns; User authentication; Impersonation attack; Feature Ranking
計畫中文摘要	近年來軟硬體技術持續地飛速成長，全球智慧型手機使用者的數量預計在2021年達到約40億用戶。智慧型手機常用來儲存一些隱私資料，因而利用智慧型手機使用各種雲端服務所伴隨而來的資安風險，益發引人重視。例如破解文字或圖形等密碼抑或是利用肩窺(Shoulder Surfing)等方式竊取密碼等等，進而非法侵入手機竊取個人隱私資料。本團隊近幾年利用智慧型手機內建感測器收集使用者行為資訊，研發出非侵入式(non-intrusive)使用者驗證機制(authentication mechanism)，名為「MLock」(Mobile Lock)的驗證機制雛型(prototyping)。目前MLock 3.0藉助雲端伺服器來進行模型訓練與測試，各方面之效能已達世界標準，然距離商品化仍需解決下列工程議題。其一、使用者在上傳個人行為資料至雲端的過程中，仍有資料被竊取的風險。因此，模型訓練與測試應當朝手機端發展，然受限於手機端有限的硬體資源，訓練模型的設計必須更加輕量化。其二、人類行為經常隨時間發生變化，所以必須探討因應行為變化(behavior change)有效率的重新訓練策略(retrain strategies)。其三，任何一種基於行為模式開發的認證機制都應當探討各種惡意攻擊(如impersonation attack，也就是假冒攻擊)下此機制的強韌性(robustness)，而目前學界對手機認證機制這方面的探討極為欠缺。因此本團隊計劃在第一年通過開發輕量化的重新訓練方法來解決行為變化問題，接者在第二年以及第三年解決假冒攻擊問題。在第二年中，本團隊透過初步的研究發現了單一受害者弱特徵(weak features)的存在，且此類弱特徵容易受到惡意攻擊的模仿。為了建立一個有力於抵禦惡意攻擊之模型，本團隊將透過增加受害者和攻擊者的數量來模擬不同的情境，並依據上述的多種情境分別建立第二年以及第三年的模型，以找出可能受到任何類型攻擊之多位受害者間的共同弱特徵(common weak features)。
計畫英文摘要	Since the advent of smartphones, with the rapid growth of hardware and software technologies, smartphones become more important in our daily life, reaching over 4 billion users by 2021. Smartphones are often used to store some private data, which sometimes may be at risk of being stolen and used maliciously. While smartphones bring convenience, they are also accompanied by risks, and these risks have expanded to become information security issues. For example, methods such as brute force attacks or even shoulder surfing could be adopted to illegally obtain individual private data. In recent years, our team has utilized built-in sensors on smartphones to collect user behavioral data to develop a prototype of a non-intrusive authentication mechanism called “MLock” (Mobile Lock). The current MLock 3.0 relies on cloud servers to conduct model training and testing. While the performance measures have reached global standards, there remains a few engineering challenges before the team is able to turn the prototype into a product. First, when the user uploads individual behavioral data to the cloud, the risk of data theft remains. Therefore, model training and testing need to be developed on smartphones. In order to conduct these processes on the smartphone, the design of the model must be light to accommodate the hardware constraint of the smartphones. Next, human behavior evolves over time. To take the change in behavior into account, the team needs to consider efficient retrain strategies. Finally, the robustness of any authentication based on behavioral patterns should be measured against any form of malicious attack (e.g. impersonation attacks); however, there is a gap in the literature regarding authentication mechanisms on smartphones. The team plans on addressing the

	behavior changes issue in the first year by developing light-weight retrain methods. The team plans on addressing the impersonation attack issue in 2nd and 3rd year. In the 2nd year, the team will find the weak features of a single victim that easily mimicked by some malicious activity. In order to build a robust model, team will complete the model built in 2nd year by increasing the number of victim and attackers to find the most common weak features that might appear in several victims, and could be attacked by any kind of attackers.
計畫概述	請概述執行本計畫之目的及可能產生對人文、社會、經濟、學術發展等面向的預期影響性(三百字以內)。 ※此部分內容於獲核定補助後將逕予公開
	本研究計畫所提的以輕量級演算法改進智慧裝置使用者驗證系統效率及安全性之技術研發,對於社會方面,可防止使用者因使用上不便利性而選擇關閉手機的安全認證機制，造成的安全漏洞，強化手機上的安全性;在學術發展方面,本研究計畫提出改善模型訓練效能的策略, 將為後續研究者提供一個新的改進驗證系統效能的方向。