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；智慧型手錶；資訊安全；行為特徵；使用者驗證；多重驗證；線上學習；遷移學習；領域適應
計畫英文關鍵詞	Smart device; Smartphone; Smart watch; Information Security; User Authentication; Multiple authentication; Online Learning; Transfer Learning; Domain Adaptation
計畫中文摘要	隨著電子硬體及軟體技術的蓬勃發展和行動網路的普及，使智慧裝置(Smart Devices)在市場上快速發展，並逐步取代家用電腦和筆記型電腦，隨著這股熱潮也使得行動應用(Mobile Application)，成為軟體產業中重要發展方向。然而，行動應用帶來龐大的商機也導致許多新型態資訊安全議題，例如近年興起的行動支付應用，電子商務研究團隊eMarketer研究追蹤與預估2018年擁有智慧型手機用戶中的34.9%比例，會在智慧型手機上使用行動支付，又根據市調報告指出，約莫60%-80%的智慧型手機使用者因貪圖方便，會長時間關閉智慧型手機上的安全認證機制，這也讓冒名者很輕易的能對手機中的重要資料進行擷取或盜用甚至是行動支付的盜刷，使得智慧裝置原本存在的個人隱私與個人資料保護的資安議題，衍生成更為嚴重的個人財產安全問題。因此，智慧型手機上的安全性需要提升與強化。根據本團隊近年執行的研究計畫與學術發表的論文，已針對智慧型手機及智慧型手錶研發基於使用者行為的驗證機制；我們發現驗證機制除了考量驗證準確率之外，應將系統之使用性(Usability)與可靠性(Reliability)也納入考量中，如在建構使用者預測模型階段，不適合讓使用者重複太多次相同的收集動作，花費太多時間在資料收集上，這會造成使用者覺得枯燥導致降低使用意願，並且驗證機制也須因應使用者隨時間的操作行為改變，進而自動更新預測模型，否則將造成預測效能降低，此外單一的行為模型驗證系統有一定效能上之極限，由於穿戴式裝置將會成為未來行動裝置的趨勢，將引進智慧型手錶，透過結合操作智慧型手機之腕部行為，藉此提供多重驗證方法，以提升驗證系統之精確度。故本研究計畫將針對智慧型手機使用者認證機制提出一個以多種學習策略增進智慧型裝置使用者驗證能力之技術方法，藉此提升認證機制的使用性與可靠度，提高使用者的使用意願與維持驗證效能。
計畫英文摘要	With the rapid advances in electronic hardware and the popularity of mobile networks. It's not only making Smart Devices rise rapidly in the market and gradually replaced personal computers and laptops but also leads Mobile Applications to become an important direction of development in software industry. However, the huge business opportunities brought by mobile applications have also led to many information security issues. For example, the mobile payment application. A research team called eMarketer, they estimating 34.9% of smartphone users in 2018 will use mobile payment on smartphone and also according to the market report, about 60 %-80% of smartphone users will turn off the security authentication mechanism on their smartphones because of their convenience. This allows imposters can easily capture or steal sensitive or private information from the smartphone or even using mobile payment. Which makes existing personal privacy issues more serious. Therefore, the security protection on smart devices needs to be enhanced. Our team focus on the development of the nonintrusive authentication methods based on users' behavior in the past few years. Besides the authentication accuracy, we found that the usability and reliability of a smartphone user authentication system also has to be considered. As an example, it's not proper for requesting user to repeat the same actions as many times and also makes collecting time too long. Moreover, the authentication system must automatic update the predicted models, because the habitual behaviors of the smartphone user maybe change over time. The authentication accuracy may drop down if the predicted model

	does not keep the latest. In addition, a single behavioral model authentication mechanism has certain performance limits. As wearable devices will become the trend of future mobile devices and in order to improve the accuracy of the authentication system. Smart watches will be imported to provide multiple authentication mechanisms by combining the wrist behavior of using smartphones. Therefore, this project will propose a method for enhancing the authentication capability of smart device by using various learning strategies for the smartphone user authentication mechanism, thereby improving the usability and reliability of the authentication mechanism and increasing the user's willingness to use also maintain authentication performance.
計畫概述	請概述執行本計畫之目的及可能產生對社會、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
	本研究計畫所提的基於多種學習策略改善智慧型手機使用者驗證機制之模型建構效率研究，對於社會方面，可防範使用者因操作或使用上的不方便而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，本研究計畫研究實務上之行為模型建構效能的影響，將為後續研究者提供一個新的思考或可改善效能的方向。