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；使用者驗證；行為特徵；資訊安全；對抗性攻擊；對抗樣本；假冒攻擊；弱特徵；特徵排名
計畫英文關鍵詞	Smart device; Smartphone; User Authentication; Behavioral Biometric; Information Security; Adversarial Attack; Adversarial Examples; Impersonation Attack; Weak Features; Feature Ranking
計畫中文摘要	隨著科技的發展，近年來人工智慧(Artificial Intelligence, AI)越來越廣泛地應用於安全性(Security)和可靠性(Reliability)至關重要的領域，如行動支付等包含個人敏感訊息之應用，根據電子商務研究團隊eMarket於2021年的統計全球使用行動支付的人數比例已達44.6%，顯示了行動支付於近代社會中的重要程度。而研究團隊考量到過往智慧型手機所使用的安全認證機制如文字密碼(Text Password)仍有機會被有心人士透過肩窺(Shoulder Surfing)的方式破解，因此團隊於近年執行的研究計畫發表的學術論文皆致力於研發基於使用者行為的非侵入式使用者驗證機制。然而，在AI發展的同時，模型被攻擊所造成重大傷害的風險也在持續上升當中，透過本團隊的初步實驗，我們得知所研發之驗證機制會受到其對抗性攻擊(Adversarial Attack)：假冒攻擊(Impersonation Attack)，也就是惡意人員可透過模仿使用者行為藉以混淆系統的驗證。因此，研究團隊將透過不同的情境進行三年研究，確保能研發一個更加穩健且可靠的身份驗證機制，以抵禦來自各方攻擊者的假冒攻擊。第一年度，團隊將透過單一受害者與單一攻擊者的情境，嘗試進行初步實驗以找出攻擊者易模仿的受害者特徵，確認假說：弱特徵的存在性。第二年度將透過單一受害者與多位攻擊者的情境，建立一個專屬於當前受害者的模型，以保護此受害者預防來自所有攻擊者的假冒攻擊，提升驗證機制的穩健性。第三年度，透過多位受害者與多位攻擊者的情境，團隊將增加模型的可用性，確立最終所建立的通用模型適用於所有使用本驗證機制的用戶。
計畫英文摘要	In recent years, the development of science and technology affects the popularity of the artificial intelligence. It is applied to many areas where security and reliability are critical, such as mobile payment and other applications, which may contain sensitive personal information. According to the statistics provided by the e-commerce research team eMarket in 2021, the number of people who use the mobile payment in this modern society has reached 44.6%. Some traditional authentication methods such as passcode, are prone to malicious attack by unauthorized users through the activity so-called “Shoulder surfing”. Some research aim to build a non-intrusive user authentication mechanism based on user’s behaviour. On the other side, as the artificial intelligence becomes more complex, the risk of system failures causing significant harm rises. Based on the preliminary experiments we have conducted, the adversarial attacks have impact to the authentication mechanism. Malicious users intend to fool the authentication mechanism by mimicking legitimate users’ behaviours. We called this specific adversarial attack, an “impersonation attack”. Based on the aforementioned background, we propose several different experimental scenarios to build a model, which is robust and reliable against impersonation attacks from various attackers. In the first year, we are going to conduct preliminary experiments, to find out the characteristics of the victim, which is easy to be mimicked by the attacker, through “one victim to one attacker” scenario. The outcome of the first year will be the confirmation of the existence of weak features. In the second year, we are going to build a robust authentication model to protect a specific victim against the impersonation attacks from all attackers, through “one victim to many attackers” scenario. In the third year, we are going to improve the usability and flexibility of the model. The model will be