

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。

(二) 計畫英文摘要。(五百字以內)

總計畫：Developing the Cloud Technology to Support Users Authentication on Handheld Devices and Virtual Laboratory Deployment.

Handheld devices become increasingly popular due to many ubiquitous and innovative applications emerging rapidly in recent years, which have made profound impacts on people's daily life. These new applications also raise new security threads to our information assets as mobile users tend to access services available on the Cloud. There is an urgent call for new security mechanism to improve the security level in additional to existing ones. There is another trend to deploy scientific experiments, such as network intrusion laboratory, over the Cloud in order to take the advantage of the elasticity of the underlying Cloud infrastructure. The idea of "Virtual labs" brings promise of letting students engage in experiments that cannot be done otherwise. Chances are, however, a single IaaS (Infrastructure as a Service) vendor may not be able to offer sufficient resources to support a full blown experiment such as "DDOS attack". Multi-Cloud technology, therefore, is a useful alternative when situation like this to happen. This proposal comprises of three subprojects entitled "a handheld device authentication mechanism for Cloud client" (Subproject I), "On the Design of a Cloud Service for Virtual Labs" (Subproject II), and "on the development of a cloud infrastructure with high elasticity and high availability" (Subproject III). Subproject I, addresses the first issue when a handheld device is used to access a Cloud service. This subproject relies on the services supported by both Subproject II (multi-Cloud accessing) and Subproject III (IaaS). Subproject II, on the other hand, addresses the virtual lab issues and it also relies on the IaaS services provided by Subproject III.

Keywords: *Cloud security, User authentication, Virtual laboratory, Multi-Cloud services*

子計劃一：A handheld device authentication mechanism to improve security level of Cloud services via securing the Cloud clients

As the performance and the features rapidly increased, handheld devices (i.e. smartphones) are used not only for communicating purposes but also for other applications, such as Cloud services accessing. Several surveys show that smartphones are used more frequently for various applications other than telecommunication. These new applications raise new security issues whether the security mechanisms of current handheld devices are sufficient to protect sensitive data stored in the devices or Cloud platforms. The current protection mechanisms of these devices are usually based either on PIN codes, passwords, or biometric-based methods, such as fingerprints or face recognition. Both fingerprints and password entry are intrusive in the sense that they require explicit action from the user, which is not convenient in frequent use. The same surveys also show that most (60%-80%) users choose to turn these verification features off simply because of its inconvenience. On the other hand, the sensitive information stored in Cloud platforms is generally protected by the passwords, PINs, or security codes; however, the password-based authentication methods used on mobile devices have a shoulder-surfing issue. Then, the handheld devices may become one of the major security vulnerabilities of Cloud platforms. To improve the security of the handheld devices, non-intrusive authentication mechanisms are desirable. We observe that people tend to have unique ways of holding and operating their handheld devices. Consequently, we found that the two sensitive apparatus of handheld devices, namely the orientation sensor and the touchscreen, are capable of capturing the unique behavioral biometrics while the user is engaged in relatively stationary activities, such as holding the device to perform apps. We therefore propose a non-intrusive authentication mechanism based on these two sensors. Applying the proposed mechanism, the Cloud services could defense the most illegal accessing through the handheld devices.

Keywords: *Cloud security; Handheld device; Smartphone; Non-intrusive authentication mechanism*