## 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 BYOD Security Technologies for Enterprise Cloud**

The dramatic growth of cloud computing services and mobility trends, in terms of 3/4G availability and smart devices, facilitate a trend called “BYOD” (Bring Your Own Device), which means the employees use their own devices also during their working time. However, the use of their devices for both personal and working activities opens to new security threats to face for IT organization, e.g. data leakage, data theft and regulatory compliance. The existing methods, e.g. mobile application management, which only manages access permission on a single mobile application. Then, this method may create a few security weaknesses, for example, collude issue. Beside, mobile devices are easy to be stolen, lost and have the shoulder surfing issues. Moreover, BYOD security must pay attention to user authentication techniques on mobile devices. This proposal comprises of three subprojects entitled “A Research of Cloud-Based Security Technology for BYOD” (Subproject I), “A Poses Adaptive Authentication Mechanism Based on Behavioral Biometrics Obtained from Mobile Devices” (Subproject II), and “Supporting Highly Reliable Software Service on OpenStack Using Integrated Failure Detection of Physical Machines and Virtual Machines” (Subproject III). Subproject I proposes the solution to address the first issue, that not only applies data centric-information flow control mechanism to avoid collude issues, but also provides static app analysis to improve BYOD security. Subproject II, on the other hand, proposes the solution of the authentication issues of mobile device, developing a new non-intrusive authentication mechanism based on their behavior information on the mobile device. Furthermore, the authentication service also is integrated to Subproject I’s security management platform. In order to improve the reliability of software services on enterprise cloud, Subproject III provides the monitor and recovery technologies to physical machines and virtual machines.

***Keywords:*** *Enterprise Cloud; Bring Your Own Device; User Authentication; Mobile Device Management; High Availability Services*

## 子計劃二：A Poses Adaptive Authentication Mechanism Based on Behavioral Biometrics Obtained from Mobile Devices

With the rapidly improved information technologies and the widely used Internet services, mobile devices, such as smartphone, become widely used apparatuses for accessing various types of digitalized information. Consequently, the security issue of access control becomes an important research topic of mobile devices and information systems. The existing access control methods of mobile devices and information systems are primary password-based; however, this method has drawbacks of passwords forgotten and/or stolen. To resolve the drawbacks of text-passwords authentication method, Herzberg had proposed two-factor authentication method in 1964. We believe that it is a possible solution to propose behavioral-biometrics-based authentication mechanisms as the second factor since it is nonintrusive and difficult to be forged or mimicked. However, our recent research found that a smartphone user may have multiple behavioral patterns caused by varying operating poses (e.g. sitting and standing); and then, the performance of an authentication model would be decreased. In this project, we therefore adopt behavioral biometrics obtained from smartphone sensors, namely touch screen and orientation sensor, to propose an operating poses adaptive authentication mechanism. Finally, a prototyping, namely MLock, will be implemented by applying the proposed mechanism. It could be used to authenticate an owner of mobile devices in the enterprises adopted a policy, namely Bring Your Own Device (BYOD). The prototyping could also be integrated with password-based authentication method of general information systems to build two-factor or multi-factor authentication mechanisms for improving system security.

***Keywords:*** *Mobile device; Behavioral biometrics; Non-intrusive authentication mechanism; Multi-factor authentication; Multiple operating poses*