Communications of the CCISA
Vol. 23 No. 2 Apr. 2017

基於開放源碼雲端運算架構之高彈性駭客攻防教學平台之設計與評估

許建隆[1、4、5]、蔡昇宏[2]、林子煒[3*]
[1,2]長庚大學資訊管理學系、[3]長庚大學企業管理研究所、
[4]明志科技大學視覺傳達設計系、[5]長庚紀念醫院
[1]clhsu@mail.cgu.edu.tw、[3]d0340003@stmail.cgu.edu.tw

摘要

網路科技進步的轉變，逐漸讓資訊安全受到重視，倡導資訊安全 教育也就越重要，傳統刻板的文字敘述及投影片解說的教學，這樣所得到的學習效果是有限的。此外，駭客攻防技術之教學除了原理與工具之介紹外，亦需要一個實境模擬的駭客攻防環境，讓學生可以透過此環境，演練駭客攻防技術並評估學習成效，以提昇其學習效果與意願。本研究基於開放源碼技術以及 OpenStack 技術，設計並建置一個雲端運算之駭客攻防教學平台，並建構相關駭客攻防教材。此平台分為二個部分，分別為駭客攻防原理教學平台，以及駭客實境模擬攻防平台。對於學生而言，可以達到理論與實務操作之學習，用以培訓具實務攻防能力之人才。對於教師而言，能以低成本的概念製作出具有高彈性與可用性的教學平台，快速建構雲端化駭客攻防教材，以及快速且大量佈署並監控駭客實境模擬攻防環境，以了解學生理論與實務操作之學習成效。此平台將可作為資訊安全攻防人才培訓之雲端培訓基地。此外，本研究進一步運用科技接受模型，以及開源雲端運算平台分析之相關文獻，設計一個適用於雲端駭客攻防教學平台之科技接受度研究模型，探討使用者對於此類平台之接受度研究。本研究結果顯示出系統的娛樂性能提升使用者使用教學平台之意圖，知覺有用性能夠提升使用者使用教學平台之態度。藉由統計分析結果能瞭解學習者對於使用雲端教學平台進行資訊安全與駭客攻防學習之接受度，亦將提供未來教師與資訊人員建立雲端駭客攻防教學平台或推動相關教學平台開發之重要參考依據。

關鍵詞：雲端運算、資訊安全、駭客攻防、數位學習、科技接受模式

Design and Evaluation of a High Elastic e-Learning Platform for Ethical Hacking Based on Open Source Cloud Computing Architecture

Chien-Lung Hsu [1、4、5], Sheng-Hung Tsai [2], Tzu-Wei Lin[3*]
[1、2]Department of Information Management, Chang-Gung University
[3]Graduate Institute of Business and Management, Chang-Gung University
[4]Department of Visual Communication Design, Ming-Chi University of Technology
[5]Administration, Chang-Gung Memorial Hospital
[1]clhsu@mail.cgu.edu.tw, [3]d0340003@stmail.cgu.edu.tw

Abstract

The changing of network and technological progress has gradually alert the attention information security and information security education. Traditional stereotypical narrative teaching has limited effect on learning. In addition, to present the hacker attack and defense technology, it needs a reality simulated hacker attack and defense environment for students. By drill of hacker offensive and defensive techniques, we can evaluate the effectiveness of learning and enhance the willingness of learning. This study is based on open source and OpenStack technology, design and build a cloud computing platform for teaching and construction of the relevant hacker attack and defense materials. This platform is divided into two parts, namely the principles of teaching platform hacker attack and defense as well as hackers reality simulation platform. As for the students, they can achieve learning theory and practical operation, trainings with offensive and defensive capabilities of the personnel. For teachers, they are able to produce low-cost concept teaching platform with high flexibility and availability of the cloud to quickly construct a hacker attack and defense materials, as well as a large number of rapid deployment on environment and also monitoring the hacker attack and defense reality simulation environment for students both theoretically and practically. This platform will be used as base practice ground for cloud information security attack and defense training. In addition, this study uses technology acceptance models as well as open source cloud computing platform analysis and design a suitable model for science and technology acceptance cloud teaching platform of hacker attack and defense from user acceptance perspective. The results of this study shows entertainment of the system can enhance the users' intention of platform using. Users can also enhance the perceived usefulness of using teaching platform attitude. By statistical analysis, teaching learners to use this cloud platform for information security and acceptance of hacker

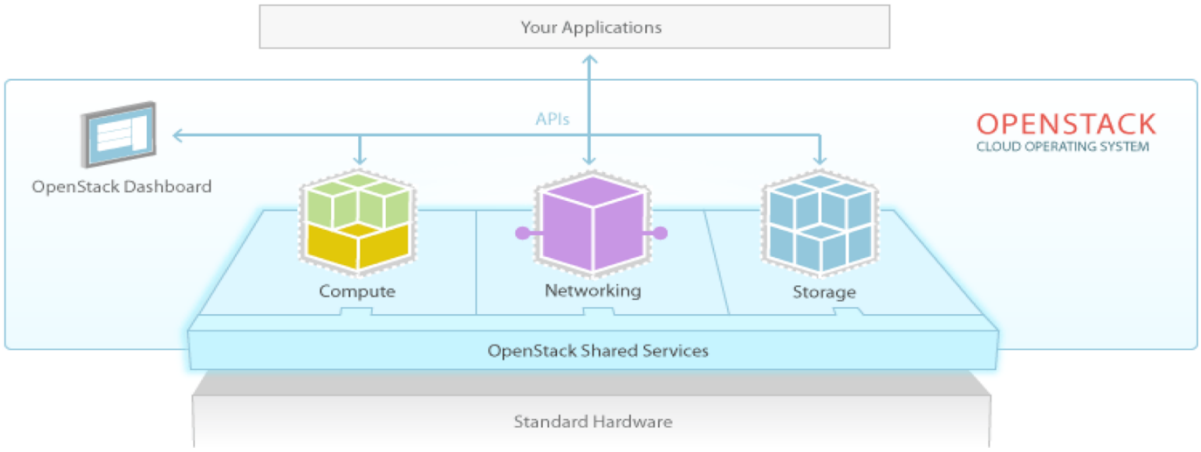
attack and defense learning will also provide teachers with information to develop cloud teaching platform and important reference on related works.

Keywords: Cloud Computing, Information Security, Ethical Hacking, e-Learning, Technology Acceptance Model

壹、前言

雲端運算(Cloud Computing)是指運用一種基於網際網路的運算形式，藉由此形式可共享軟硬體資源與資訊可按照需求提供給電腦或其他裝置，具有高彈性與高延展性之特性，可以提供使用者所需要的功能[2]。美國國家標準技術研究所(National Institute of Standards and Technology，NIST)提出 The NIST Definition of Cloud Computing 中，雲端運算服務模型主要分為基礎設施即服務(Infrastructure as a Service，IaaS)、平台即服務(Platform as a Service，PaaS)、軟體即服務(Software as a Service，SaaS)。基礎設施即服務主要提供硬體資源給使用者，包括機器運算、儲存服務、網路頻寬等基礎設備之整合服務，利用硬體資源透過虛擬化技術將運算、儲存和網路等資源抽象化，實現整體的自動化和資源管理流程的改進，還可以對外提供高動態並且靈活的基礎架構服務。2009 年 B. Sotomayor et al.學者[13]指出，隨著 IaaS 越來越受歡迎，各種工具與技術不斷湧現，能夠幫助企業將基礎架構改變。但由於各種技術不斷的發展，系統管理者要挑選適合的 IaaS 環境是很困難的。2012 年 G. Von Laszewski et al. 學者[7]所提出多個雲端架構比較中，已幫助系統管理者針對不同 IaaS 框架進行評估，由此評估可得知 OpenStack 可包含許多不同的套件，比起其他 IaaS 平台更不容易進行佈署，但也代表其可擴充性和支援程度是截至目前為止最好的。2013 年 I.M. Abbadi et al. 學者[1]所提到 OpenStack 雲端軟體的調度機制，能夠提高我們以前對雲端的信任，妥善的雲端調度機制是可以同時考慮用戶需求和基礎架構的性能。2012 年 X. Wen et al. 學者[14]協助比較 OpenStack 與 OpenNebula 這兩套熱門雲端軟體之間差異，幫助評估雲端運算架構的優劣。

OpenStack 由美國國家航空暨太空總署和 Rackspace 公司一起合作研發的雲端 IaaS 運算軟體，同時是一個自由軟體與開放源碼的程式。OpenStack 是雲端操作系統，能在整個資料中心控制運算、儲存和網路資源的資源池。系統管理者只需透過儀表板，就能夠即時控制，同時可以透過 Web 賦予使用者資源，進行資源的管理，如圖一所示。



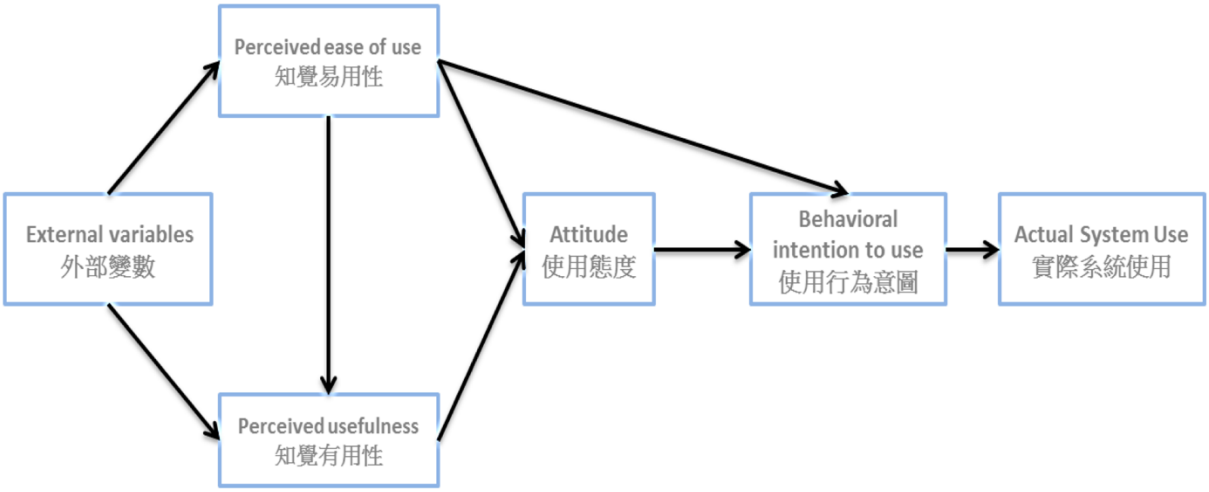
圖一：OpenStack 基本架構[16]

數位學習(e-Learning)廣泛的定義是學習者利用數位媒介來進行學習的過程，Gartner Group 美國市場研究機構認為數位學習屬於遠距教學的一種，使用衛星廣播與互動電視等來進行授課程教學，但主要是以網際網路的介面來傳輸數位教材。2011 年 Y. Park et al.學者[11]所介紹移動化學習的定義，闡述其特點，並且與電子學習進行對比，未來能夠隨時進行學習是一種趨勢。美國政府為了讓使用者不致浪費在數位學習上的投資，推薦使用學習元件的參考模式 SCORM (Sharable Content Object Reference Model)，並提出「同一教材內容可在不同平台上操作，同一平台可操作不同廠商開發的教材」的要求，此即為相互操作性，可讓各種產品與工具教材之間的相互流通，不斷升級社交媒體與各種技術漸漸地改變學習的方式，個人化的獨立學習環境使得學習者能夠更融入學習。

MOOCs (Massive Open Online Course，大規模開放線上課程)起源於開放教育資源與關聯主義的思潮。2013 年 T.R. Liyanagunawardena et al. 學者[8]提到，現今已有很多研究者積極投入 MOOCs 案例研究。MOOCs 參與的方式跟一般大學的課程內容很類似，目前採不給予學分但會給予學習者學習證書。傳統課堂的設計主要是針對一小群的學生人數來對應相對的單位教師，但 MOOCs 希望是給網路上不特定的參與者，因此學習者的規模非常龐大。運用 MOOCs 能方便處理大眾的互動和回應，像是同儕審查、小組合作等，還可透過即時客觀的線上評量系統加以測驗，讓整體教學模式得到更佳的學習效果。2011 年 R. Kop et al.學者[6]指出，一個成熟的電子學習用戶，透過 MOOCs 進行學習的參與水平是比較高的。2013 年 T.R. Liyanagunawardena et al. 學者[8]針對 2008 年至 2012 年 MOOCs 的文獻進行回顧研究，得知 MOOCs 能夠提供教育環境內前所未有的大規模潛在教學成效。2005 年 S. Graf et al.學者[5]進行各學習平台的研究，認為 Moodle 優於其他教學平台。2009 年 T. Martín-Blas et al.學者[10]證實 Moodle 能有效幫助學生學習，達到增強學習的效果，並針對使用過的學生對 Moodle 系統提供的功能回饋進行研究，學生反應非常良好。Moodle 是一套開放源碼的平台，提供教育

者、管理者和學習者具有單一平台且功能強大，注重資訊安全，豐富的系統來創建個人化的學習環境。使用者可以自己補足套件不足的地方，其中作業發佈模組的功能多樣，可以讓教師評閱，還可建立測驗模組、互評模組。Moodle 官方表示會持續維持開放源碼的模式，相信每一個教育環境，都可以讓每一個參與者在良好回饋機制下受惠[15]。本研究根據 2008 年 C. Romero et al.學者[12]研究中所提出完整數位學習數據分析的理念，利用學習數據分析技術來探討數位教學互動與學生發展學習的效果關係，希望能夠幫助教師有更創新的教學方式，來幫助學生學習。因為當利用學習數據分析技術，指導教師假如發現學生參與課堂的頻率逐漸減少，指導教師就可及早介入、避免教學效果不彰，當學生在某個教學章節需要花費很多時間重複學習，或是該章節的測驗成績不好，就代表教學章節太過困難或是教師講解不夠清楚，這時候教師就可以即時重新設計教學方式。依 Moodle 官方統計，目前全球已經有超過 7900 萬用戶使用，使其成為世界上使用最為廣泛的學習平台。

科技接受模式(Technology Acceptance Model, TAM)由 F.D. Davis et al. [4]於 1989 年提出，以理性行為理論(TRA)為基礎，其目的希望能解釋與預測人們對資訊科技使用的影響因子，其模型如圖二所示。



圖二：科技接受模式 TAM [4]

TAM 主要是用來探討外部的因素對於使用者的內部信念(Beliefs)、意向(Intentions)及態度(Attitudes)的一些影響，進而影響資訊系統的使用情形，TAM 還探討使用者面對新科技時，是否可以接受新科技設備及使用新科技的系統。TAM 提出使用態度會影響使用者的重要原因，而態度主要影響分為知覺的有用性(Perceived usefulness)與知覺的易用性(Perceived ease of use)。

1. 知覺有用性主要的定義為軟體使用者會傾向使用他們所認為的，可以幫助工作上面做得更好更完整的軟體。
2. 知覺易用性：當潛在軟體使用者相信某一種軟體是有用處的，但是若軟

體使用者所需花費的心力與時間遠超過軟體系統使用上所帶來的效益，則軟體使用者就會傾向不採用此軟體系統。

本研究參考 2001 年 J.W. Moon et al. 學者[9]提出發現知覺有用性和知覺易用性兩個因素不足以解釋網路使用者動機，藉由科技接受模式加上娛樂性(Playfulness)構面，由 J.W. Moon et al.提出衡量娛樂性的面向分別為：

1. 專注：在娛樂狀態，使用者注意力會集中在活動上。當使用者使用系統進入娛樂的狀態時，使用者會很專注。
2. 好奇心：當使用者在使用系統的過程中，會引起使用者的好奇心，讓使用者想進行探索。
3. 享受：當使用者在使用系統的過程中，會引起使用者享受的感覺，使其感到愉悅。

2007 年 T. Ahn et al. [3]提出線上零售平台的使用者行為意圖，其研究除了在 TAM 加上娛樂性，另外加入系統品質、資訊品質與服務品質。此研究模型結果為娛樂性對於態度與行為意圖有正向影響的關係，此意味著使用者會持續採用線上零售商，對於服務本身的有趣性，也會因為娛樂性因素而對線上零售廠商產生忠誠度，因此娛樂性也是使用者決定採納線上零售網站系統的關鍵因素。

本研究提出建構與評估基於開放源碼雲端運算架構之高彈性駭客攻防教學平台，期望能夠提供教師與學生更完整且具高彈性之開放源碼雲端運算架構的駭客攻防教學平台，基於開放源碼的架構下，希望能運用靈活彈性且可程式化的雲端教學平台，進行具有彈性佈署之教學環境。本研究設計「基於開放源碼雲端運算架構之高彈性駭客攻防教學平台」，包含以下 7 點特性:1.基於開放源碼，整體建置價格較低、2.結合雙模組平台(教學平台與攻防演練平台)、3.實務攻防操作練習，具有互動性、4.雲端操作架構不受場域、時間或環境的限制、5.高彈性攻防演練平台具有大量快速佈署機制、6.根據學生進度狀況，可調整攻防演練系統難易度、7.未來資源不夠時，快速彈性擴充主機。本研究將使用 T. Ahn et al.學者[3]提出科技接受模型結合系統品質、資訊品質、服務品質與娛樂性進行評估。

貳、系統設計

本研究希望設計出基於開放源碼雲端運算架構之高彈性駭客攻防教學平台，來幫助學生進行學習，培育更多的資訊安全人才，替未來全國資訊安全環境打造出可用之兵。

2.1 系統建置流程

本研究採用雛型法(Prototyping)來進行平台設計，雛型法是一種反覆討論的開

發流程，使用者與系統設計者經由不間斷的重覆討論、設計、實作、測試、使用者評估並進行修正，實作出滿足使用者需求之教學平台。本研究因涉及資訊人員、學生與教師三種職業，故本研究已徵求以上人員之意見，以求平台需求的正確完整性。

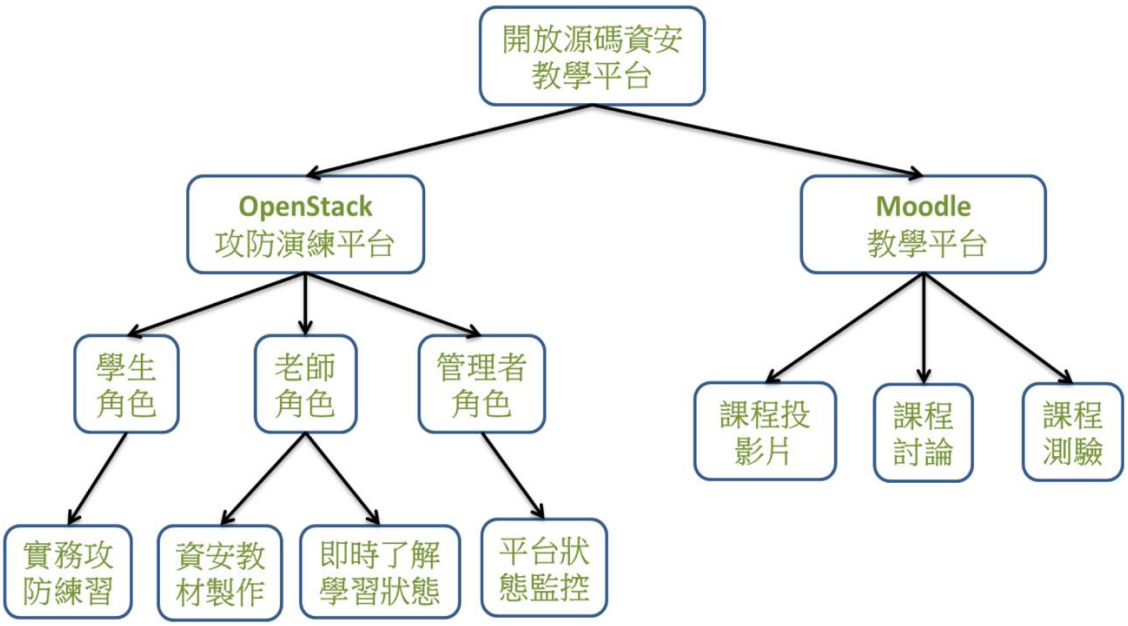
2.2 系統架構與設計

綜合前述文獻回顧與教學需求訪談，本章節會針對本研究的系統架構與系統設計之考量點進行詳細說明。

2.2.1 系統架構

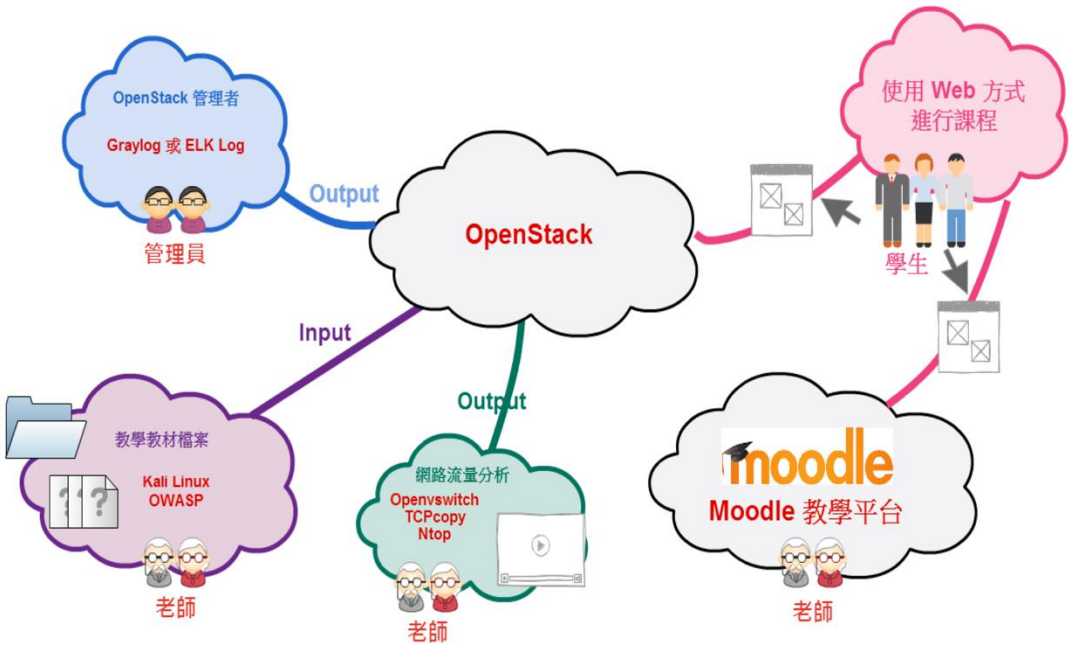
本研究之開放源碼駭客攻防教學平台，整體架構包含 Moodle 教學平台與 OpenStack 攻防演練平台兩大平台系統，如圖三所示。開放源碼駭客攻防教學平台無論任何時間、任何地點與任何設備上都可以運行，平台架構包含以下功能：

1. Moodle 教學平台：此平台能幫助學生進行課程回顧、解決教學時間限制並且能即使掌握學生學習進度，教學平台包含以下三種系統模組：
   (1) 課程投影片：提供教師上傳教學投影片或影片，學生隨時能上網進行學習。
   (2) 課程討論：提供學生們討論空間，利用課後時間學生們可以與教師進行互動。
   (3) 課程測驗：教師可直接利用線上測驗，確認學生學習狀態，並即時修正教學方式。
2. OpenStack 攻防演練平台：此平台希望透過實務攻防演練，來幫助學生進行學習。藉由登入使用者進行分類，包含學生、教師、管理者，以下詳述三種角色之差異：
   (1) 學生：學生只需藉由網頁瀏覽器就可以隨時隨地登入此平台並進行課程學習，不需使用大量系統效能就可進行操作攻防教學系統，達到即時性且真實的資訊安全學習。
   (2) 教師：可在此平台隨時隨地上傳課程的教材檔案，只需要從網頁瀏覽器就可以登入此平台進行大量攻防教學系統的佈署調整，快速切換上課教材，並藉由攻擊練習流量分析、日誌分析達到即時了解學生學習的進度。
   (3) 管理者：藉由此平台系統管理者可以即時了解，教學過程中系統所使用的資源狀態。並即時監控調整伺服器使用量，更可以彈性分配伺服器，避免不當調度所造成的資源浪費。



圖三：開放源碼駭客攻防教學平台架構圖(本研究)

本研究預期建構之平台主要為輔助教師與學生進行資訊安全駭客攻防學習過程，提供教師上傳客製化教材，教師可從平台進行大量佈署，教師只需要準備一份數位教材，即可供全班進行課程。本研究藉由虛擬化技術將實體伺服器便成為大量的資源池，可以彈性調度伺服器資源。為了可以讓學生在無時間限制且快速便利的環境下學習，因此，所有系統皆可使用瀏覽器進行操作，也可以使用手機平板進行連線，如圖四所示。

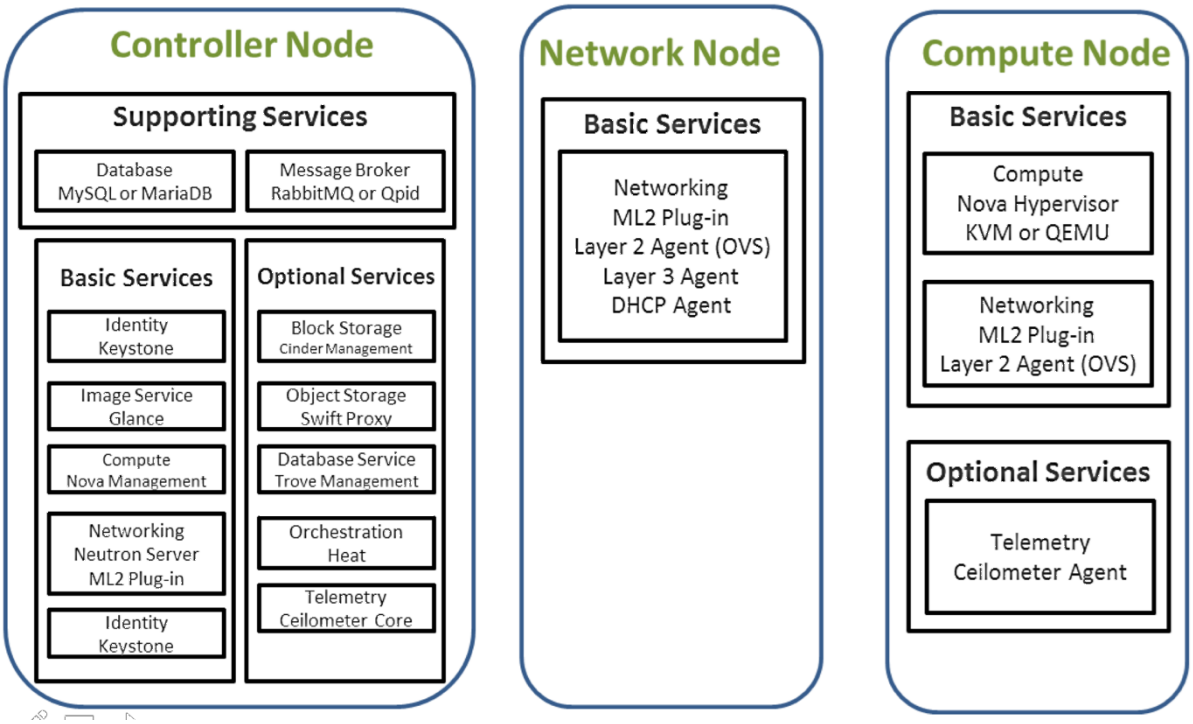


圖四：開放源碼駭客攻防教學平台架構圖(本研究)

2.2.2 系統設計

本研究為了增進學生對於資訊安全學習的臨場體驗，設計了高彈性的 OpenStack 攻防演練平台，可以讓學生體驗資訊安全學習的樂趣。本研究結合 Moodle 教學平台和 OpenStack 雲端攻防演練平台，Moodle 教學平台使用獨立實體主機進行安裝，OpenStack 雲端攻防演練平台主要會藉由數台實體主機進行架設，針對不同研究需求可進行微調。本研究 OpenStack 攻防演練平台基本架構使用一台 Control Node、一台 Network Node、三台 Compute Node 來進行實作，如圖五所示。

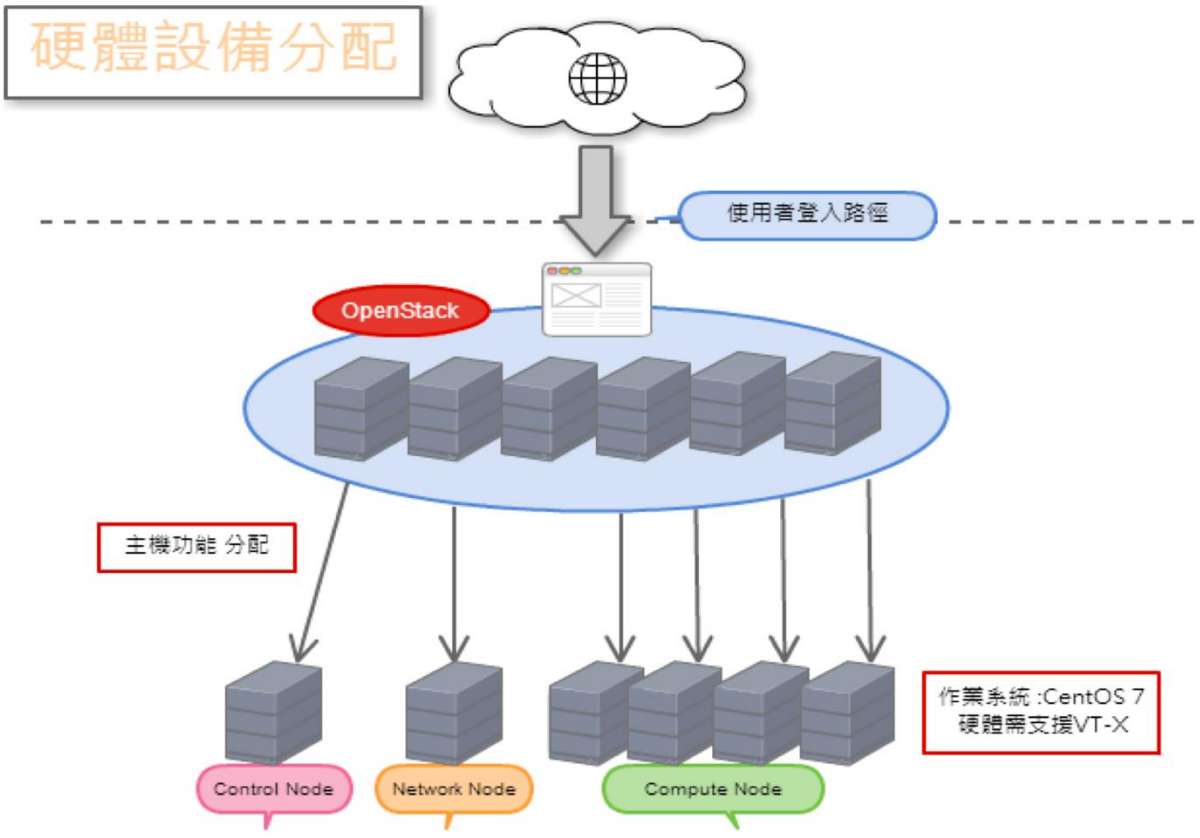
1. Controller Node：運作 Keystone、Glance、管理運算的部分和網路服務，並運作網路 plugin 以及 Horizon 儀表板。其中包括一些支援性的服務，例如 SQL 資料庫、訊息佇列(Message Queue)和網路時間協定(NTP)。
2. Network Node：運作 Networking plugin 和一些租戶(Tenant)網路提供的代理，並提供 switching、routing、NAT 和 DHCP 服務，這個節點也可處理租戶虛擬機實例的外部網路(Internet)連接。
3. Compute Node：運作 Compute 的 hypervisor 部分，此部分將操作 tenant virtual machines 或實例。預設情況下，Compute 使用 KVM 作為 hypervisor，運算節點也可以運行 Networking plugin 和代理，它們連接租戶網路到虛擬機並提供防火牆(Security Groups)服務。



圖五：OpenStack Node 服務說明

本研究參照 OpenStack 官方建議，共有以下六種架構可以進行選擇性建置：通用型雲端運算、運算型雲端運算、儲存型雲端運算、網路型雲端運算、多區域型雲端運算與混合雲端運算。經由分析各類型架構與評估所需之需求，決定採用通用型雲端運算架構，因 OpenStack 通用型雲端運算架構被普遍使用者認為是建構雲端運算起點，該架構被設計為平衡所有元件與整體運算環境中不強調某一個特定領域。本研究評估雲端運算架構設計必須針對運算、網路、儲存等元件作必要公平權衡，所以本研究查證通用型雲端運算實務上已有各種建置案例，因此，本研究最終採用通用型雲端運算架構。本研究預計使用五台實體主機進行設計，作為攻防演練平台驗證，整體硬體設備分配如圖六所示，雖然通用型雲端運算並不會特別針對任何特定套件或功能提供優化調整性能，若日後某方面效能不足時，管理者還是可以進行調整以及增加實體伺服器。

本研究期望從 OpenStack 教學平台得到學習者的回饋，來做即時性分析，藉由收集學生攻防演練之封包資訊，做更深入封包解析成有用的資料，接著藉由封包資料經過資料視覺化加工處理，經由網頁方式進行顯示至學習進度儀表板，可以讓教師更了解學生的學習進度。



圖六：OpenStack 教學平台硬體設備分配(本研究)

2.3 系統成果

本研究設計之平台分成 Moodle 教學平台與 OpenStack 攻防演練平台。

1. Moodle 教學平台：教師可以事先將課程教材投影片與相關影片或工具上傳至平台。可針對不同的課程做區分，學生可針對需求選擇課程，進入課程後可以看到課程儀表板，教師可以在這個頁面進行課程的資訊公告；學生也可以藉由 Moodle 課程內的連結，直接連線到 OpenStack 攻防演練平台；學生經過課程學習後，教師可以藉由 Moodle 教學平台考試，即時的對學生進行測試驗證教學成果與成效。
2. OpenStack 攻防演練平台：此平台可以讓學生直接藉由網頁方式登入，讓學生可以隨時進行學習，如圖七所示。該登入網頁是藉由 OpenStack 儀表板套件 Horizon 進行修改調整，由 OpenStack 身分識別套件 Keystone 進行統一的登入身分認證。

根據不同登入帳號的權限，教學平台網頁則會顯示不同的選項，本研究主要分為學生、教師與管理者三種角色，每種角色登入後皆有不同的網頁畫面。

圖七：OpenStack 攻防演練平台登入網頁(本研究)

(1)學生：此角色只要直接利用網頁方式輸入個人帳號登入，就可以即時進行攻防演練，整體的介面如圖八所示。

圖八：OpenStack 攻防演練平台學生登入畫面(本研究)

在左方選單中，專案選項內學生較常使用的系統功能為運算和網路，運算中包含以下元件：

A. Instance 雲實例：列出所有的虛擬機，可以對虛擬機進行操作，例如遷移，刪除等。

B. Volumes 雲硬碟：顯示用戶使用與創建空間。

C. Image 映像檔：顯示可使用的映像檔，可以即時上傳鏡像，只需要知道 Image 是何種格式。

D. Key pair：Key pair 對能在鏡像啟動的時候加入到映像檔中，不過前提時該鏡像必須包含 cloud-init，使用者需要為 Project 建立至少一個 Key pair，如果您已經通過外部工具創建了 Key pair，您可以將其導入 OpenStack，在一個 Project 內的多個實例可以共用一個 Key pair。

E. 安全組：用來決定哪些網路流量能流至實例。安全組中包含了一組防火牆策略，被成為安全組規則。

F. 浮動 IP：可以為了虛擬主機分配一個 Public IP。

G. API 存取權：利用程式進行 API 呼叫，啟動調整 VM 設定。

網路中包含以下元件：

A. 網路拓樸：可以清楚了解主機的網路狀態。

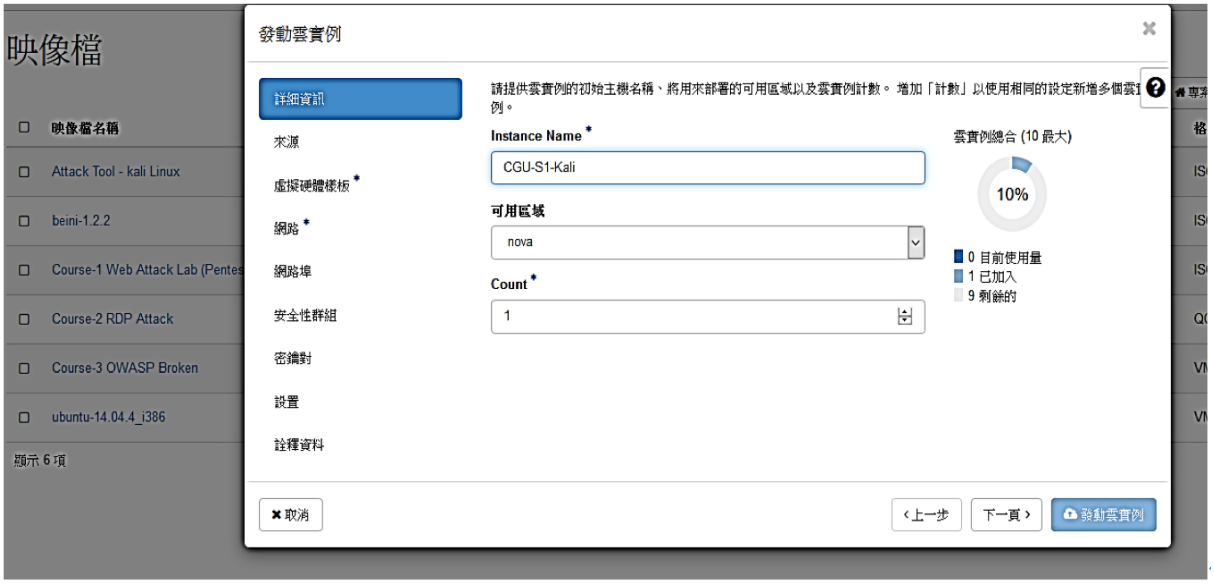
B. 網路：可新增獨立網路，讓主機使用。

C. 路由器：用來將不同網路進行間接。

對學生而言，藉由此平台來學習資訊安全攻防練習是容易上手的，因為教師可以事先將設計好的資訊安全課程教材上傳，學生只需依照需求至映像檔內選擇即可，如圖九所示。

圖九：OpenStack 攻防演練平台映像檔(本研究)

啟動虛擬主機只需要按照步驟，依序設定名稱、啟動數量、映像檔來源、虛擬硬體樣板、網路等資訊，就可以快速開啟 VM，來操作流程，如圖十所示。



圖十：OpenStack 攻防演練平台啟動虛擬機流程(本研究)

當啟動虛擬主機時，如圖十一所示，畫面可以撰寫客製化 Script，讓

虛擬主機系統啟動時，就會自動執行客製化的設定。

圖十一：OpenStack 攻防演練平台客製化腳本(本研究)

當虛擬主機啟動後只要藉由 OpenStack 架構內的主控臺就可以進行操作，主控臺採用 noVNC 技術，學生可直接由瀏覽器支援 HTML5 方式操作虛擬機，如圖十二所示。

圖十二：OpenStack 攻防演練平台主控臺(本研究)

(2)教師：主要管控不同學生 Project 狀態，如圖十三所示。不但能直接從網頁上傳攻防教材虛擬主機檔案，還可直接在攻防演練平台內進行虛擬主機的調整，此平台依學生不同的使用情形，教師可以直接大量進

行佈署攻防虛擬機，給予不同的學生使用。

圖十三：OpenStack 攻防演練平台教師管控學生專案(本研究)

(3)管理者：主要管控整個攻防演練平台的狀態，並可針對不同課程或不同使用者進行新增 Project，每一個 Project 是各自獨立使用，藉由管理者能夠完整將每一個 Project 使用過的虛擬 CPU 時數和記憶體時數統計出來，並計算出硬碟每 GB 的使用時數和使用的容量，進一步分析不同課程於攻防演練平台內的資源使用率，如圖十四 所示。

圖十四：OpenStack 攻防演練平台管理者畫面(本研究)

本研究整合 Moodle 與 OpenStack，教師可藉由 Moodle 教學平台來進行測驗，即時針對教學過程中不足的資料進行補充，靈活度相當高，另外也能用來評估學生課程活動的紀錄，並藉由圖形化的方式來顯示學生在每一個課程中的活動報告，而且 Moodle 教學平台可以建立很多個課程，剛好整合 OpenStack 攻防演練平台不同的 Project 進行討論。

本研究藉由 Moodle 建置教學平台的優勢為：1. Moodle 為原生教學平台；2. 開放源碼；3.內建各種教學與評量模組；4.隨時隨地的線上學習討論；5.降低成本。本研究藉由 OpenStack 建置攻防演練平台的優勢為：1. OpenStack 為原生雲端平台；2.開放源碼；3. 同時間大量佈署主機，靈活調配主機；4.隨時隨地的線上攻防練習；5.降低成本。本研究期望能夠讓教師與學生們能有更好的資安學習環境，目前有整理相關資安攻防工具，教師可以針對需求將資安攻防工具匯入攻防演練平台內。

1. 整合型工具：Kali Linux、HoneyDrive
2. 弱點掃瞄：Nessus、OpenVAS、Nexpose、SearchDiggity
3. 網站掃瞄：Nikto、Wikto、Burp Suite、Paros Proxy
4. 網路探測與分析：Nmap Security、Wireshark、Tcpdump

5. 密碼分析：AirCrack、Cain and Abel、John the Ripper、Ophcrack
6. 資訊收集：Metasploit、Metago

為了讓 OpenStack 管理者或教師能夠更清楚瞭解整個 OpenStack 的狀態與學生學習的狀態，本研究有整理相關的攻防演練平台管理層面的工具，方便日常的維運。

1. 雲端平台：OpenStack、CloudStack、Ezilla、VMWare
2. 資料分析：ELK、Splunk、Netwitness
3. 系統與網路管理：MRTG、Cacti、Nagios、Zabbix
4. 網路流量分析平台：Ntop、Wireshark、Tcpdump

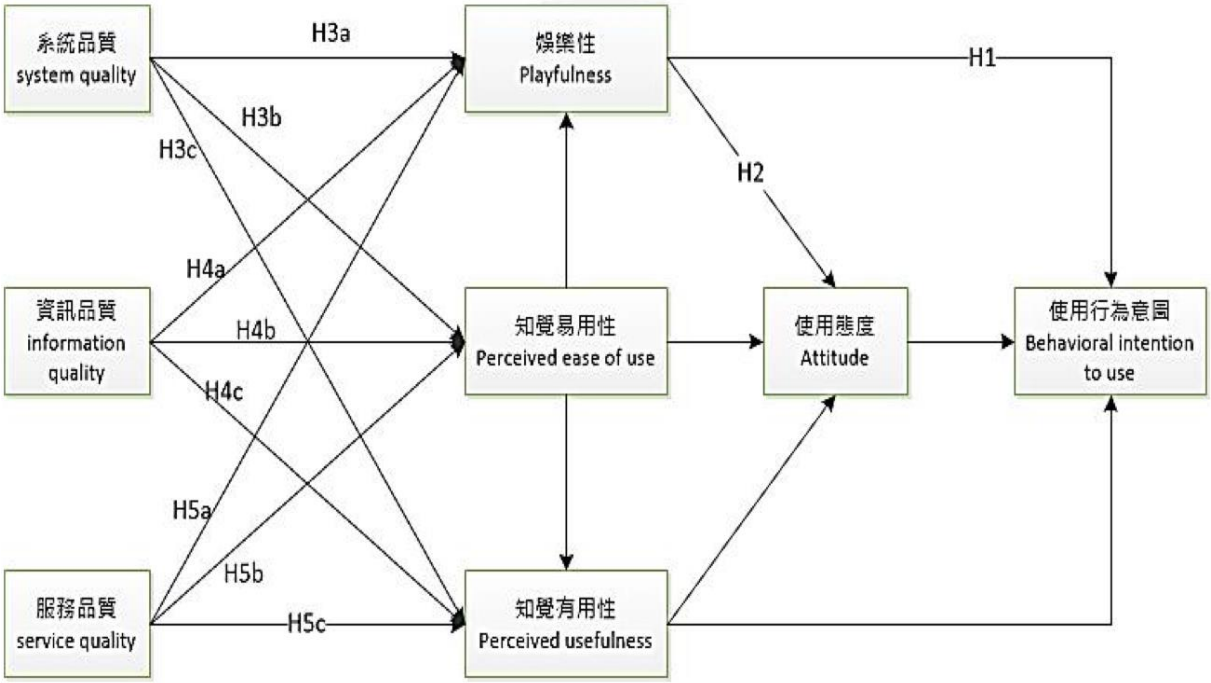
根據日本資安分析師於台灣資安大會中揭露日本資訊安全人才培育藍圖，目前日本企業從事資訊安全領域 IT 技術人員有 23 萬名，但是距離企業所需要資安人才數量，還缺少 2.2 萬人。從這些數據可以看出資訊安全人才的供給能力，目前還無法填補企業資安人才缺口，尤其在資訊安全 IT 技術人員中還有 14 萬名需要加強資訊安全技術能力。行政院宣布「資安政策 2.0」中，提出資訊安全人才培育的相關做法，但可能還有許多需要克服的障礙需思考加以突破，因此未來資訊安全的技術能力培養是全世界都將面臨的問題。本研究基於開放源碼雲端運算架構之高彈性駭客攻防教學平台，希望能夠成為培養資訊安全駭客攻防一個良好管道，以幫助資訊安全人才的培育。

參、系統驗證與使用者接受度調查

本研究以實際建置系統與操作的方式進行驗證使用者的科技接受度，包括實驗過程的設計、樣本的取得、問卷內容的設計及分析。

3.1 研究模型

本研究以 T. Ahn et al. [3]於 2007 年提出修改後之科技接受度為研究模型架構做基礎，針對本研究開放源碼雲端運算架構之高彈性駭客攻防教學平台進行評估，研究模型如圖十五所示。



圖十五：研究模型圖(本研究)

3.2 研究變數與假說

根據前述之研究模型，本研究提出研究假說如下：

假設 H1：資安教學平台的娛樂性會正向影響使用者的使用行為意圖。

假設 H2：資安教學平台的娛樂性會正向影響使用者的使用態度。

假設 H3：資安教學平台的系統品質對使用者正向的影響，可以分成以下三種假設。

H3a：資安教學平台的系統品質會正向影響使用者的娛樂性。

H3b：資安教學平台的系統品質會正向影響使用者的知覺易用性。

H3c：資安教學平台的系統品質會正向影響使用者的知覺有用性。

假設 H4：資安教學平台的資訊品質對使用者正向的影響，可以分成以下三種假設。

H4a：資安教學平台的資訊品質會正向影響使用者的娛樂性。

H4b：資安教學平台的資訊品質會正向影響使用者的知覺易用性。

H4c：資安教學平台的資訊品質會正向影響使用者的知覺有用性。

假設 H5：資安教學平台的服務品質對使用者正向的影響，可以分成以下三種假設。

H5a：資安教學平台的服務品質會正向影響使用者的娛樂性。

H5b：資安教學平台的服務品質會正向影響使用者的知覺易用性。

H5c：資安教學平台的服務品質會正向影響使用者的知覺有用性。

本研究問卷問題項均以 Likert 7 點尺度衡量，「1」代表非常不同意，「7」代表非常同意，回答分數越高，表示越同意題項之描述內容。各問項均請受訪者針對實際使用心得進行填答。

3.3 問卷調查

本研究的受試者主要針對具有資訊背景的大學生、在職研究生、教師與資訊人員，主要考量的三個因素。其一是大學以上學歷對於電腦知識的程度落差較小；年輕人也比較喜歡嘗試新鮮事物，較能接受新的學習方式；本研究的平台主要以教學為目的，因此，受試者需要有學生與教師背景。因此，本研究受試者會以國內具有資訊背景的大學生、在職研究生、教師與資訊人員為主，進行本教學平台的科技接受度模型做探討。

本研究的問卷使用線上問卷方式，填寫問卷前會出現本研究平台操作說明影片以及展示本教學平台的功能與特色，接著受試者會實際藉由瀏覽器來操作本教學平台的攻防演練平台與介面，以完成實際體驗的問卷作答。最後實驗總共收到 113 份有效問卷，本研究利用敘述統計的方式來進行分析，說明問卷樣本的資料特性與分布情形。

3.4 資料分析

本研究在問卷回收後使用 SPSS 軟體進行資料分析與假說檢定。分析方面包含信效度分析，並採用「迴歸分析」進行整體模型分析。

3.4.1 信度與效度分析

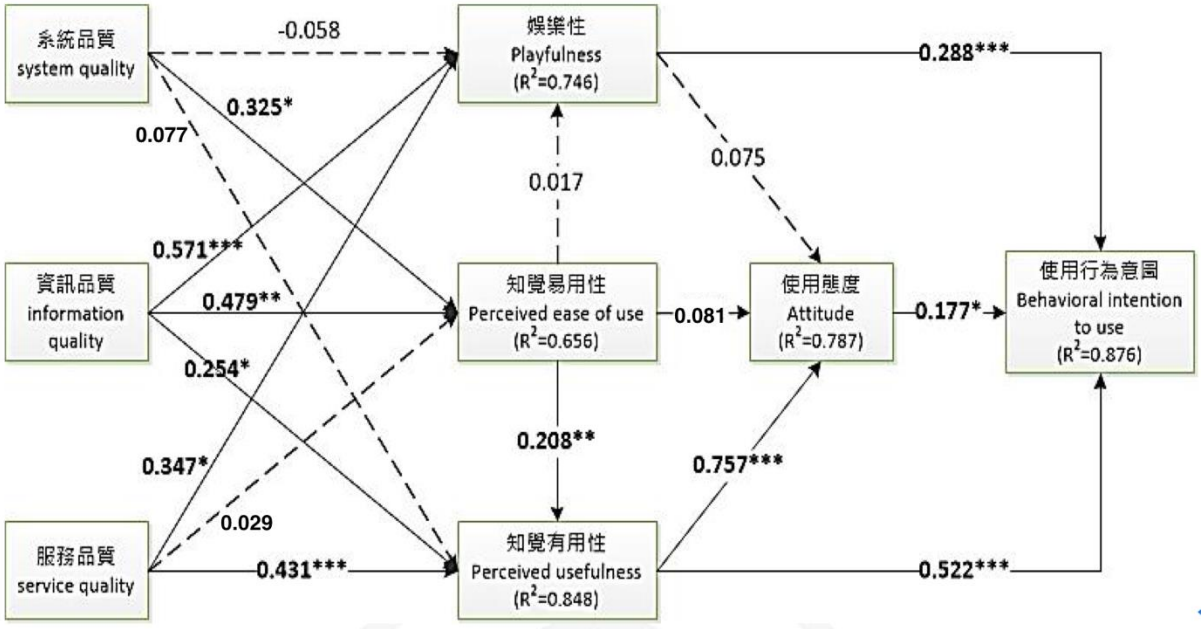
本研究信度分析使用 Cronbach’s α 係數來檢定信度大小，測量問卷一致性，當其值愈大則信度愈高。問卷量表除知覺易用性為中信度，其餘各構面 Cronbach’s α 值 0.9 以上，皆有大於 0.7，顯示問項具有良好的高信度。

本研究效度分析使用因素分析來檢定效度大小，測出衡量特質和功能，當其值愈大則效度愈高。進行因素檢測前，進行 KMO 與 Bartlett 檢定。KMO 係數值高於 0.5 即可進行因素分析，本研究問卷量表的 KMO 值為 0.939，且 Bartlett 檢定達顯著，因此本問卷資料適合進行因素分析。

因素分析收斂效度是使用兩種不同衡量方式來衡量同一構面，若相關程度很高，代表其具有收斂效度。因此，收斂效度需要同一構面之因素負荷量需大於 0.5 與組合信度必須大於 0.7。本研究因素分析結果符合條件。

3.4.2 路徑分析與假說檢定

本研究使用 SPSS 軟體迴歸分析進行檢定提出的 11 個研究假說，並依照檢定結果繪製路徑分析圖，並加上 R^2 解釋力來觀察實質的因果意義，如圖十六所示。



圖十六：路徑分析圖(本研究)

(*P < 0.05;**P < 0.01; ***P < 0.001)

根據路徑分析顯示娛樂性的 R 平方為 0.746，代表有 74.6%的娛樂性可由系統品質、資訊品質、服務品質、知覺易用性這四個構面來解釋。知覺易用性的 R 平方為 0.656，代表有 65.6%的可由系統品質、資訊品質、服務品質三個構面來解釋。知覺有用性的 R 平方為 0.848，代表有 84.8%的知覺有用性可由系統品質、資訊品質、服務品質、知覺易用性四個構面來解釋。使用態度的 R 平方為 0.787，代表有 78.7%的使用態度可由娛樂性、知覺易用性、知覺有用性三個構面來解釋。使用行為意圖的 R 平方為 0.876，代表有 87.6%的使用行為意圖可由娛樂性、使用態度、知覺有用性三個構面來解釋。

3.4.2 路徑分析與假說檢定

本研究之開放源碼雲端運算架構之高彈性駭客攻防教學平台根據檢定結果歸納出幾點說明：

1. 研究結果顯示資安教學平台的「娛樂性」與使用者的「使用行為意圖」有正向的影響。當資安教學平台具有「娛樂性」，則使用者使用的意圖會越高。
2. 研究結果顯示資安教學平台的「娛樂性」與使用者的「使用態度」無明顯影

響。推論可能由於教學平台是教學為目的，因而在「娛樂性」構面中呈現不顯著之情形。

3. 研究結果顯示資安教學平台的「系統品質」與使用者的「知覺易用性」有正向的影響，「系統品質」與使用者的「娛樂性」、「知覺有用性」無顯著影響。推論由於教學平台的好壞只會影響使用者易用程度，並無明顯影響使用者娛樂感受與學習上有用程度，因而在「娛樂性」、「知覺有用性」構面中呈現不成立之情形。
4. 研究結果顯示資安教學平台的「資訊品質」與使用者的「娛樂性」、「知覺易用性」及「知覺有用性」有正向的影響。當資安教學平台的資訊品質越好，能有效增加使用者在使用平台的「娛樂性」、「知覺易用性」與「知覺有用性」。
5. 研究結果顯示資安教學平台的「服務品質」與使用者的「娛樂性」及「知覺有用性」有正向的影響，「服務品質」與使用者的「知覺易用性」無明顯影響。推論由於受測者具有基本資訊水平，服務品質並不會影響平台易用程度。因而在「知覺易用性」構面中呈現不顯著之情形。

肆、結論與未來研究方向

現今社會無足夠資安專業人才進入職場，而導致資訊安全人力短缺，起因為現有社會環境並未重視資訊安全，因此，資訊安全需要全民一起重視，而從小就推廣資安領域好處與優勢，才能深植於學生心中。現今網路科技發達，一個良好學習平台，能夠讓教師規劃課程更容易，讓學生學習更有效率，資訊安全不再是傳統刻板的文字敘述及投影片解說的教學，必須讓學生學習達到最佳化及了解實務的處理狀況。因此，本研究平台可以讓教師更容易規劃課程以及即時了解學生學習狀況，快速調整教學進度。學生可以在學習中透過互動的方式體驗實作過程以及更有效率了解資訊安全情境。達到實際體驗效益。本研究根據科技接受度重要構面之外，整理架構與資料分析結果後，顯示對平台的使用者而言，教學平台的「娛樂性」，確實能提升使用者採用本研究教學平台之意願。

本研究限制為受測者來源經由網路發送線上問卷之方式，僅限學校內在職研究生、大學生、教師與資訊業界服務的朋友與同事們填寫。受限於特定的職業群組，可能無法代表所有使用者之意見。由於資訊安全領域有一定技術門檻，大部分的受測者填具問卷時大多依其對資訊安全的認知回答，與實際為資訊安全從業人員經驗有程度差距，因此，會有些許的落差。

本研究提出開放源碼雲端運算架構之高彈性駭客攻防教學平台設計與評估研究，針對未來研究建議如下：本研究將 Moodle 與 OpenStack 兩個平台結合運用，後續研究者可結合更多不同開放源碼之系統，達到教學目的，而且本研究主要針對資訊安全領域，後續研究者可以針對其目標學習族群加以探討

[誌謝]

本研究接受財團法人資訊工業策進會贊助，計畫名稱：「可規模化資料去識別化分析技術成效評估研究(GARPD3F0011)」；科技部經費補助：MOST-105-2221-E-182-053、MOST-105-2923-E-182-001-MY3 以及 MOST-104-2221-E-182-028。

參考文獻

[1] I.M. Abbadi and A. Ruan, "Towards Trustworthy Resource Scheduling in Clouds," *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 6, 2013, pp.973-984.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "A View of Cloud Computing," *Communications of the ACM*, Vol. 53, No. 4, 2010, pp.50-58.

[3] T. Ahn, S. Ryu and I. Han, "The Impact of Web Quality and Playfulness on User Acceptance of Online Retailing," *Information and Management*, Vol. 44, No. 3, 2007, pp.263-275.

[4] F.D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*: *Management Information Systems*, Vol. 13, No. 3, 1989, pp.319-339.

[5] S. Graf and B. List, "An Evaluation of Open Source E-learning Platforms Stressing Adaptation Issues," *5th IEEE International Conference on Advanced Learning Technologies* (*ICALT 2005Kaohsiung*), 2005, pp.163-165.

[6] R. Kop, H. Fournier and J.S.F. Mak, "A Pedagogy of Abundance or a Pedagogy to Support Human Beings? Participant Support on Massive Open Online Courses," *International Review of Research in Open and Distance Learning*, Vol. 12, No. 7, 2011, pp.74-93.

[7] G. Von Laszewski, J. Diaz, F. Wang and G.C. Fox, "Comparison of Multiple Cloud Frameworks," *Proceedings - 2012 IEEE 5th International Conference on Cloud Computing* (*CLOUD 2012*), 2012, pp.734-741.

[8] T.R. Liyanagunawardena, A.A. Adams and S.A. Williams, "MOOCs: A Systematic Study of the Published Literature 2008-2012," *International Review of Research in Open and Distance Learning*, Vol. 14, No. 3, 2013, pp.202-227.

[9] J.W. Moon and Y.G. Kim, "Extending the TAM for a World-Wide-Web Context," *Information and Management*, Vol. 38, No. 4, 2001, pp.217-230.

[10] T. Martín-Blas and A. Serrano-Fernández, "The Role of New Technologies in the Learning Process: Moodle as a Teaching Tool in Physics," *Computers and Education*, Vol. 52, No. 1, 2009, pp.35-44.
[11] Y. Park, "A Pedagogical Framework for Mobile Learning: Categorizing Educational Applications of Mobile Technologies into Four Types," *International Review of Research in Open and Distance Learning*, Vol. 12, No. 2, 2011, pp.78-102.
[12] C. Romero, S. Ventura and E. García, "Data Mining in Course Management Systems: Moodle Case Study and Tutorial," *Computers and Education*, Vol. 51, No. 1, 2008, pp.368-384.
[13] B. Sotomayor, R.S. Montero, I.M. Llorente and I. Foster, "Virtual Infrastructure Management in Private and Hybrid Clouds," *IEEE Internet Computing*, Vol. 13, No. 5, 2009, pp.14-22.
[14] X. Wen, G. Gu, Q. Li, Y. Gao and X. Zhang, "Comparison of Open-source Cloud Management Platforms: OpenStack and OpenNebula," *Proceedings - 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery* (*FSKD 2012*), 2012, pp.2457-2461.
[15] Moodle Official Website, https://moodle.org/.
[16] OpenStack Official Website, https://www.openstack.org/.

[作者簡介]

許建隆博士分別於 1997 年與 2002 年取得臺灣科技大學資管系碩士與博士學位，自 2011 年 8 月起擔任長庚大學資管系教授，並自 2013 年 8 月起兼任系主任一職，亦兼任長庚大學 RFID 物流與供應鏈應用學程與資訊與醫療安全學程之召集人、中華民國資訊安全學會之理事與會員委員會主任委員。專長領域包括智慧家庭、行動商務、電腦與通訊安全、資訊安全、應用密碼學、健康照護、數位版權管理、自動辨識技術、數位鑑識。

蔡昇宏先生於 2016 年取得長庚大學資訊管理學系碩士學位，其研究興趣為網路安全、資訊安全、密碼學。目前於麟瑞科技股份有限公司擔任工程師。

林子煒先生分別於 2011 年與 2013 年取得長庚大學資訊管理系學士與碩士學位。2013 年 8 月，林先生於中央研究院資訊服處服研發替代役。2014 年 9 月，進入長庚大學企業管理研究所修讀博士學位迄今。研究領域包括密碼學、資訊安全、物聯網應用安全及雲端運算應用安全等。