結合協同合作之誘捕式雲端網路安全防護

張朝旭	陳博智	謝維哲	劉韋伸	陳光祥	林寶翔
國立聯合大學	國立聯合大學	國立聯合大學	國立聯合大學	國立聯合大學	國立聯合大學
資訊管理系	資訊管理系	資訊管理系	資訊管理系	資訊管理系	資訊管理系
副教授	助理教授	學生	學生	學生	學生
cschang@ nuu.edu.tw	pcchen@ nuu.edu.tw	spydo97@ gmail.com	peanut12345638@ gmail.com	blackhumor1@ gmail.com	day6235@ gmail.com

摘要

雲端運算(Cloud Computing)的出現，使得網路服務使用設備愈趨於輕薄且具行動性，而所提供的服務亦趨於便利而多元化，導致現階段經由網路使用服務的潮流愈來愈盛行。由於雲端是個新興的科技，安全防護尚不完整，而雲端運算的服務必須是穩定的而強健，假使雲端安全有漏洞進而遭受攻擊，其所提供的服務就可能會中斷；亦或使用者的資料可能會遭到外洩，造成龐大的損失傷害，因此雲端的安全防護極為重要。一般而言，雲端運算的使用門檻低，使用者在雲端透過一個入口主機即可獲取想得到的服務，但服務來源可能來自同地域以及不同地域的服務主機，如同一個跨地域的區域網路。然而這些跨地域服務主機相互溝通時，可能因遭受攻擊如：DDos 攻擊，而無法順利連結合作以提供服務，進而造成雲端主機癱瘓。

因此，本研究擬提出一雲端網路攻擊偵測系統來解決上述的問題，以確保雲端網路安全。此系統模組可分為分流偵測系統、偽裝偵測系統、弱點分析系統與協同合作系統。其中，分流偵測系統偵測目前雲端網路上封包的傳輸行為，並觀察是否有入侵攻擊的嫌疑；偽裝偵測系統則在網路中佈建偵測點，偵測潛在的入侵攻擊；弱點偵測系統則可以偵測每台雲端服務主機的弱點，並針對那些弱點來補強，以減低安全的漏洞；協同合作系統負責將所收集的攻擊資訊與其他跨地域的協同合作系統進行攻擊資訊交換，以提供聯合防禦之能力，有效阻擋攻擊者的攻擊行為。

關鍵字：通訊安全、雲端運算、入侵偵測、網路攻擊。

1. 研究動機與研究問題

隨著資訊網路的快速發展，以及雲端運算的出現，使用者的工作平台由原先的 PC-Based 主機轉變成結合網路的雲端平台。導致使用者端之設備越趨輕巧且具行動性，因此使用雲端服務的人潮將越來越多。同時，伴隨而來的問題將是雲端傳輸應用的穩定性是否可以受到保證。由於雲端是個新興科技，安全防護目前尚不完整，而雲端運算的服務可能因此而不穩定，假使雲端安全有漏洞進而遭受攻擊，其所提供的服務就可能會中斷；亦或，使用者的資料可能會因入侵而外洩，造成龐大的損失傷害。目前個案如 Google 提供的 Gmail 服務，遭受入侵攻擊且客戶資料被外洩[1]，讓 Google 雲端服務被蒙上一層陰影，所以雲端的安全防護能力將影響使用者使用使用雲端服務的意願。因此，本研究擬針對雲端安全防護做探討，並從中找出解決之道。

雲端是一個服務平台，使用者透過一個入口主機獲取想得到的服務，但這些服務的來源，可能不只是一台服務主機而已，其中可能來自透過網路串連同地域以及不同地域的主機所形成的整合式服務主機，而這些主機串聯之後所形成的封閉網路，就像是一個跨地域的區域網路。然而這些跨地域服務主機經由網際網路相互溝通時，服務主機可能因此遭受攻擊，而攻擊者可能會透過第一台服務主機繼續找尋下一台服務主機，進而利用 DDos 攻擊這些雲端的主機，導致雲端服務癱瘓，如何在最短的時間內分辨出攻擊者，並利用防火牆擋住以保護雲端主機是非常重要的；再者，雲端是一個共享環境，雖然每個使用者看似是在獨立的環境中使用，但這些

環境很多都是透過虛擬化的技術所產生出來的，因此多台虛擬主機的資訊可能於相同的實體網路線上傳輸，所以必須要有效的隔離不同使用者使用虛擬化的平台，以避免某虛擬主機遭受攻擊時而影響其他位於同一實體主機中的其他虛擬主機所提供之服務。此外，雲端的服務主機大多使用 VMware 系統的虛擬化服務，以產生多台虛擬主機以進行服務之提供，而這些虛擬主機只有少數的實體網路出口，因此，要如何分區隔來自不同服務的資料流，以進行封包傳輸行為及流量分析，也是本研究所須探討的問題。

所以，本研究擬提出(1)分流偵測系統、(2)偽裝偵測系統、(3)弱點偵測系統、(4)協同合作系統以保護雲端網路。分流偵測系統會偵測目前雲端網路上的傳輸狀況，並觀察是否有入侵攻擊的嫌疑；偽裝偵測系統使用誘補之方式在網路中佈建偵測點，偵測潛在的入侵攻擊；而弱點偵測系統則是偵測每台雲端服務主機的弱點，針對那些弱點來進行補強，以減低安全的漏洞；協同合作系統則負責將有問題的 IP 資訊傳送給其他跨地域的協同合作系統，如此只要攻擊者攻擊其中一個地域雲，其他相關的地域雲都會阻擋此攻擊者。

2. 文獻回顧與探討

2.1 雲端運算

雲端運算是一種概念，其利用網路的無遠弗屆，讓不同地域的電腦彼此間能夠互相合作，提供更便利的服務，使用者可以使用電腦、手機等工具，透過網路就可以輕易的在雲端上做資源儲存和共享。

目前雲端平台普遍的架構是由數據中心、部屬管理軟件、監控軟件、WebSphere 應用服務[2]、資料庫、磁盤陣列[3]以及一些開放原始碼軟件、資訊處理和開放原始碼虛擬軟件所組成。雲端的優點是採取大規模便宜的服務集群得到高性能，且能使用所需最大的系統資源，不僅能提高效能，還能降低成本、突破地域性界限。對於廠商來說，廠商可以透過虛擬化技術提供不同服務，並減低成本，維護系統也較方便；而對於使用者來說，只要隨手有上網工具，便可使用雲端的服務。而雲端的缺點是其所提供的服務是按使用量付費，且執行速度會依網路速度而被限制，目前提供的服務也較少，還有許多資料安全及通訊安全的議題。整體而言，雲端就是一個減少資源消耗並具備高效能的服務平台。

雲的型態有三種，分別為公有雲、私有雲以及混合雲[4-7]。公有雲是服務供應商透過公有的網路提供外部使用者所需的服務，各個使用者一同分享該雲端供應商的資源；私有雲則透過私有的網路提供服務，針對特定的企業或組織內部成員所使用；混合雲結合公有雲和私有雲的優點，可公開的資源透過公有網路對外部使用者提供服務，而較隱密的資源則使用私有網路僅對內部成員提供服務，如此可以分擔建構私有雲的成本。

雲端運算的架構分為三層：(1)軟體即服務(SaaS)、(2)平台即服務(PaaS)、(3)基礎設施即服務(IaaS)[8]。SaaS 是供應商透過網路以租賃的方式提供軟體及應用程式，這些服務都是以網路形式進行，使用者不用管理硬體和軟體，也不需對軟體進行維護，不僅操作簡單，還能節省成本，是目前雲端運算類型中最主要的服務；PaaS 是提供網路平台的服務。使用者不需自己安裝軟體和 OS 等，透過網路利用業者提供的虛擬主機平台，就能節省軟硬體維護成本及人力管理的時間；IaaS 是將資訊基礎設施變成一種服務，提供 Server、Storage 等基礎設施，採用使用者付費的模式，用多少就付多少，以確保使用者能更有效率的取得資源。目前 Google、Amazon、IBM 等都有提供 IaaS 服務。IaaS 供應商還透過 VMware 虛擬化服務，使硬體的效益更高。

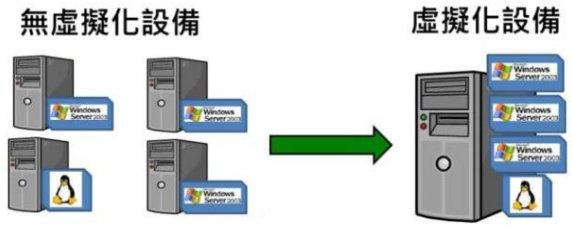
2.2 虛擬化環境

由於一般的電腦只能安裝一種作業系統，也只能提供其作業系統所提供的服務，因而產生虛擬化技術，改善了硬體資

源和應用程式的效率與可用性，在每部實體機器上執行多部虛擬機，共用單一實體電腦的資源(如圖一)，發揮最大的效率。

虛擬化的優點有很多，因為將多台主機虛擬化成少數幾台虛擬機器，不但能省電、省成本、省機房、硬碟空間，還有統一的管理介面方便集中管理，也容易做備份、轉移和升級，目前企業較多使用 VMWare 來做虛擬化。

VMWare 是一套虛擬機器[9]，可以在一部主機上同時執行多個作業系統。同時也是個強大而具有彈性的系統，不僅可以動態資源分配(DRS)[10]，監控各個資源集區的使用率，並在虛擬機間明智地配置可用資源；在硬體故障時，還能執行容錯(VMware Fault Tolerance)[11]的功能，進行即時故障切換，使其能繼續使用不會造成數據中斷或丟失的情況。當雲端服務伺服器經過虛擬化分割後將會有多台作業系統於單一硬體上，各個作業系統提供的服務都有其對外使用的 IP，因此單一硬體上就會對外對應多重的 IP，而虛擬化出來的多重服務，其外部封包皆會流進單一硬體，所以本研究為了更精準的保護雲端網路，必須要對各個 IP 封包的傳輸行為以及流量進行監測，才能準確判斷此 IP 是否為攻擊 IP，在第一時間確保雲端運算的安全性。



圖一、虛擬化設備

2.3 雲端身分識別

雲端服務如果遭到入侵，客戶的隱私資料將會被外洩，這對雲端服務造成了嚴重的威脅。雲端服務可以利用確認使用者的身分機制，只讓信任的使用者存取服務，降低不明攻擊者入侵的機會。雲端通常會透過(IDENTITY AND ACCESS MANAGEMENT,IAM)協定識別用戶身分以防止惡意攻擊[12]。以下是 IAM 的相關介紹：

2.3.1 IAM 生命週期

一個身份從被開始使用到停止使用的時間被稱為 IAM LIFECYCLE。可提供用戶所需資訊、建立認證授權的標準、使用雲端服務、監控系統安全。

2.3.2 IAM 標準和協定

可提供適合的分級方法保護雲端的資料安全，大約分為以下兩項：Security assertion Markup Language (SAML)：User 透過 Identity Provider(IdP)的認證並登入 Cloud Service Provider(CSP)，SAML 協定的用戶只須登錄一次，就可與伺服端認證，並可在用戶端和伺服端建立安全的連線；另一項協定是 Open Authentication (OAuth) protocol：User 可在不同的 CSP 之間存取服務。

2.4 雲端實例

在此列舉一個在醫療管理系統上使用雲端運算的例子[13]。傳統的醫療管理系統存在一些問題，如：硬體設備的儲存容量有限、傳統資料儲存不利於資源共享，所以可行的解決方法是採用雲端科技來開發新的管理系統 — 醫療檔案管理系統(HFMS)。HFMS 的架構(如圖二，顯示於參考文獻後)是使用私有雲的方式建置，使用者在進入雲端平台時會先經過虛擬防火牆，共享資源皆在防火牆內。坐落在不同部門和機構的虛擬儲存空間和虛擬 CPU，透過高速網路將資源分享在雲端平台上，使用者也可以使用高速網路在雲端平台上得到想獲取的資訊。此 HFMS 應用軟件可以達到最佳性能和可行性。雖然雲端運算平台可以降低醫療機構的營運成本和提高醫療機構間的效率，不同部門的服務主機相互溝通時，可能會遭受攻擊，導致醫療管理系統癱瘓，而無法運作；或者，醫療機構內部資料遭到外洩，造成重大的損失

等等。這些雲端安全性的問題極為重要，也是需要深入去探討的。

2.5 雲端常見攻擊

目前，雲端常見的攻擊方式有：IP 欺騙攻擊、ARP 欺騙攻擊、阻斷服務攻擊(Denial of Service，簡稱 DoS)、分散式阻斷服務攻擊 (Distributed Denial of Service，簡稱 DDoS)等，而攻擊又可以分為內部和外部攻擊，這些攻擊都能夠癱瘓整個雲端網路或是阻斷某台主機對外通訊的連線，使得網路主機上網緩慢甚至無法上網，以下則針對上述網路攻擊方式來介紹。

2.5.1 IP 欺騙攻擊

在發動網路攻擊的同時，攻擊者往往使用一種 IP Spoofing 欺騙的技術來躲避防禦者的追蹤，此種方式即是在傳遞的封包上面放置假造的來源端位址(Fake Source IP)，讓防禦者無法根據傳遞的封包上面之來源端位址確認攻擊者所在之處。此種欺騙方式常常伴隨著阻斷服務攻擊 (DoS)或分散式阻斷服務攻擊 (DDoS)等攻擊來進行。面對此種欺騙行為，主要的解決方法即是讓攻擊者的電腦無法竄改其來源端的 IP 位址，因此若是攻擊者是來自內部的雲端區域網路，則可透過網路設備的控制，在網路設備的傳輸埠上面綁定傳輸端(來源端)的 IP 與 MAC 位址，使雲端區網內部的傳輸者無法竄改 IP 位址，若是來自雲端外部網路，則可透過路由器(Router)來阻絕其攻擊的行為。

2.5.2 ARP 欺騙攻擊

ARP 攻擊是來自於雲端網路內部的攻擊，其運作原理是由攻擊者發送假的的 ARP 封包到網路上，尤其是送到閘道器上。其目的是要讓送至特定的 IP 位址的流量被錯誤地轉送到攻擊者所取代的地方。在 ARP 攻擊之前，攻擊者入侵雲端內部主機，以發送假的 ARP 封包資訊給閘道器，攻擊者可將被攻擊 IP 封包導向攻擊者的閘道，竊取資料後，再將封包轉送回給原位置，而攻擊者亦可不做回應或是將封包導向不存在的的 MAC 位址以達到阻斷服務攻擊的效果。此類的攻擊事件並不會對網路產生大量的傳輸流量，因此常常不易察覺，而根本解決之道即是透過監聽 ARP 傳輸需協定的運作，確保雲端區網內的主機內的 ARP 表格之正確性。

2.5.3 阻斷服務攻擊 (DoS) 與分散式阻斷服務攻擊 (DDoS)

阻斷服務攻擊(Dos)，能夠輕易的佔據目標網路頻寬，目的是使目標服務主機癱瘓，無法繼續提供使用者服務。攻擊者利用同時發送巨量的帶有資料的請求封包，一方面使目的端網路擁塞，另一方面消耗目的端主機的硬體資源，目的端主機會因無法負荷如此龐大的請求，最終當機而無法繼續提供服務。分散式阻斷服務攻擊(Distributed denial-of-service Attack, DDos)是 Dos 的一種強化式攻擊，DDos 和 Dos 的差別在於 DDos 利用網路的分散式特性，同時號召多個不同網路的主機，一同對目標主機進行攻擊，因此，DDos 的攻擊流量遠遠大於 Dos 攻擊。

面對 DoS 與 DDoS 的攻擊之解決方法可從監測雲端各個區域網路傳輸流量著手。透過流量監控軟體來長期監測網路設備上每個通訊埠的傳輸流量並記錄且統計出通訊埠檢測值，以監測每個網路主機所接收到的請求封包(Request Packet)是否有過載的 DDoS 攻擊情形發生。

2.6 雲端安全防護

雲端的安全防護大致可分成下列幾個面向。

2.6.1 弱點偵測系統

除了使服務癱瘓，攻擊者也可以利用主機作業系統的漏洞，進行盜取資料甚至是被控制為攻擊其他主機的跳板。Nessus 是一套弱點偵測系統，其可以找出雲端主

機作業系統現有的漏洞，加以分析，並提供最佳的解決方案，降低被安全的風險，避免雲端主機遭到攻擊者入侵。

2.6.2 入侵偵測系統 (Intrusion Detection System)

典型的入侵偵測系統可分為異常行為偵測(Anomaly Behavior Detection)、誤用行為偵測(Misuse Behavior Detection)。異常行為偵測統計網路中的封包，加以分析，找出異常的活動，以此可以偵測出是否有入侵攻擊的情形，然而誤判的情形相對較高，也許剛好互動頻繁的活動，就會被誤判為是一個攻擊。誤用行為偵測利用網路攻擊的行為特徵為基礎，和網路中的行為做攻擊特徵的配對，以找出正確的入侵攻擊特徵的活動，但由於配對前需要各種攻擊的行為特徵，對於最新的或未知的攻擊，因為還沒有其攻擊行為特徵值，而不能有效的抵擋。

2.6.3 誘捕系統

誘捕系統在雲端網路建置了虛擬的網路服務，目的是誘捕攻擊者進行攻擊。虛擬的服務並不會有外界使用者要求使用服務，而當有外來的服務請求時，即有可能是攻擊者，誘捕系統虛擬的服務會和普通的服務做出一樣的回應，和攻擊者進行互動，讓攻擊者誤認為其是一個可攻擊的對象，如果攻擊者進行攻擊，但其所攻擊的對象為誘捕系統所虛擬出的服務，實體的主機並不會受到攻擊的威脅，並且誘捕系統會收集攻擊者的攻擊手法等資訊，如此可以提早的發現攻擊，減少誤判的機會，還可以分析出新型的攻擊特徵行為。

IDC 公司曾做過調查[8]，調查結果顯示，在雲端運算中遇到的問題中，雲端安全是使用者最擔憂的，而資訊的安全性、性能，還有可用性是使用者最重視的。因此，為避免上述的網路攻擊與入侵同時提供遠端服務的安全性、性能以及可用性，本研究擬提出低成本、可行且不影響整體網路傳輸效率的方式來建置一個雲端網路攻擊偵測系統。為保有原來之網路傳輸效率，此系統不能放置於網路傳輸的主幹上，其必須是一旁站式系統，即置於內網中監視網路活動的主機，同時它只監視並記錄網路上異常或可能的入侵攻擊行為，因此所耗用的主機資源較少，僅需一般低成本的小型網路主機即可執行本系統，如此有效的資源使用方式將大幅提升本系統的可行性。

本研究還利用分流偵測系統、偽裝偵測系統、弱點偵測系統、協同合作系統保護雲端網路。分流偵測系統負責偵測雲端出口的流量，當有異常流量時，透過攻擊的行為偵測，找出正在進行攻擊的攻擊者，並透過防火牆阻擋攻擊者的攻擊；偽裝偵測點系統在雲端網路中對不存在的 IP 設置偵測點，當有入侵者試圖與不存在的 IP 溝通，偽裝偵測系統會替其與入侵者溝通，進而提前找出潛在的攻擊入侵者；弱點偵測系統將針對曾經遭受攻擊的主機，重點式的進行現有漏洞分析，並針對其作業系統弱點做補強動作，以減低再度遭受入侵的機會；協同合作系統負責和雲端各地域的雲聯繫，當其中一個地域的雲遭受攻擊，或者是有潛在的入侵者，協同合作系統便會告知各個地域的雲，使其都可以即時的抵擋攻擊者和入侵者的威脅。

3. 研究方法及實驗結果

本研究是針對雲端安全防護，擬定多個系統並設計系統架構圖(如圖三，顯示於參考文獻後)，深入了解封包傳遞行為，並對攻擊入侵封包進行偵測，達到安全防護的效果。首先，將對於進入雲端網路的封包(封包導入)，透過 Mirror 技術將其導到分流偵測系統內，由於此系統為旁站式系統，故不會影響雲端網路主幹上的傳輸效率，同時，分流偵測系統會檢測所有封包並紀錄其表頭內容，藉以了解封包傳遞的軌跡，進而分析雲端內部網路主機之間資料傳遞的互動性，以判斷是否遭受攻擊與入侵。如果封包傳遞的行為不具攻擊性，就會將其丟棄；如果封包經判斷為攻擊封

包，則分流偵測系統會立即告知防火牆，並更新協同合作系統內部的阻擋表(block table)，阻擋表將繼續提供弱點偵測系統進行弱點掃描，進而對其弱點做補強動作。為了更精準的偵測攻擊，本研究進一步利用偽裝偵測系統在雲端的內部網路上佈置多個偵測點，對雲端網路的封包傳的行為進行偵測，如有發現嫌疑者，便將嫌疑 IP 寫入嫌疑表，告知協同合作系統；協同合作系統會與其他跨地域或遠端的雲端網路進行溝通，並交換嫌疑表和阻擋表，讓所有雲端網路都可以即時的對入侵攻擊者進行封鎖或隔離，達到安全防護的效果。最後經由所建立的實體網路測試(聯合大學資訊管理學系網路平台)來進行結果分析，以證明本系統的可行性與有效性。

以下針對本研究之系統做詳細介紹：

3.1 分流偵測系統

SrcIP	DstIP	Type	SrcPort	DstPort	PkSi
192.168.107.147	60.199.252.181	TCP	3876	80	
60.199.252.181	192.168.107.147	TCP	80	3876	
192.168.200.60	125.233.13.11	TCP	80	2275	
192.168.200.60	125.233.13.11	TCP	80	2275	
125.233.13.11	192.168.200.60	TCP	2275	80	
125.233.13.11	192.168.200.60	TCP	2275	80	
192.168.101.63	119.167.248.148	UDP	1025	7201	
192.168.101.63	117.25.145.46	UDP	1025	7201	
192.168.101.63	61.142.208.124	UDP	1025	7201	
192.168.101.63	117.25.145.48	UDP	1025	7201	
192.168.101.63	117.25.145.52	UDP	1025	7201	

圖四、封包資訊表

封包傳輸行為與偵測流量偵測一直都是網路管理中最直觀、整體的網路使用資訊，是網路監控管理中最普遍運用在檢測攻擊的方法，根據不同的篩選條件、不同協定的統計來監看網路使用狀況與設備負擔大小，可了解各主機的運作情形與使用者行為。本研究之分流偵測系統，分析進入雲端的封包資訊，根據阻擋表，將需阻擋的 IP 封包丟棄，而將剩餘潛在攻擊的封包進行攻擊行為的比對，當流量發生異常，配合嫌疑表可能的入侵者，即時的找出目前正在進行攻擊的攻擊者。圖四是從路由器的封包 Mirror 到分流偵測系統，並記錄在資料庫的封包各項資訊。以下是分流偵測系統的兩項主要分析方法：

(1) 路由器的封包 Mirror 到分流偵測系統，並將每筆封包的資訊記錄在資料庫內，並讀取協同合作系統的嫌疑 IP 表，依據資料庫的資料對嫌疑 IP 進行比對，如確認為異常傳輸行為，則將嫌疑 IP 變更為需阻擋的 IP，並傳送給防火牆和其他地域雲的協同合作系統以利雲端全面性的防禦，最後將受攻擊的雲端主機 IP 傳送給弱點偵測系統進行其作業系統的漏洞補強。

(2) 雲端內部每個交換機連接阜(Switch Port)皆對應於雲端的各個主機，分流偵測系統針對各個 Port 進行流量的記錄並將每筆封包的資訊記錄在資料庫內，依據各個 Port 的流量計算出平均流量，並記錄其歷史流量資訊；當 Port 的流量超過標準值時，會同時比對歷史流量資訊，再判斷是否為異常活動，進而將此 IP 變更為需阻擋的 IP，傳送給防火牆和其他地域雲的協同合作系統。

3.2 偽裝偵測系統

網路上的攻擊者要攻擊雲端主機時，通常會先檢查網路中存活的主機以進行攻擊，本子系統針對雲端的網路佈置偵測點，收集攻擊者與所佈建偵測點的接觸行為，透過接觸行為的分析來確認攻擊者，進而抵擋來自攻擊者的攻擊。本子系統將會對雲端的網路進行掃描，將不存在的 IP 設置為虛擬 IP 而進行偽裝，虛擬 IP 面對網際網路的封包是由本子系統所進行回復，與存活 IP 並無不同，攻擊者同樣可以接收到虛擬 IP 所發出的回覆，而誤認虛擬 IP 是存活中的主機；藉此，進而提早找出網際網路中的攻擊者，達到保護雲端網路的功能。有關佈建偽裝偵測系統建構演算法以及偵測點釋放演算法如圖五與圖七。

3.2.1 偽裝偵測系統的建置：

```
(1)  發送 TTL=1 封包，取得 Default Gateway 的 IP 位址
(2)  發送 ARP Request 封包詢問區網活著的 ip
(3)  While(true){
   封包進來
   If(ArpReply 封包來源 ip=雲端區網 ip){
       If(ArpReply 封包目標 ip 沒有在存活表裡)
           紀錄存活 ip
       If(ArpReply=Gratuitous Arp)
           釋放偽裝中的 ip
   }
   if(IcmpReply 封包目的 ip=雲端區網 ip){
       If(IcmpReply 封包目標 ip 沒有在存活表裡)
           偽裝此 ip
   }}
```

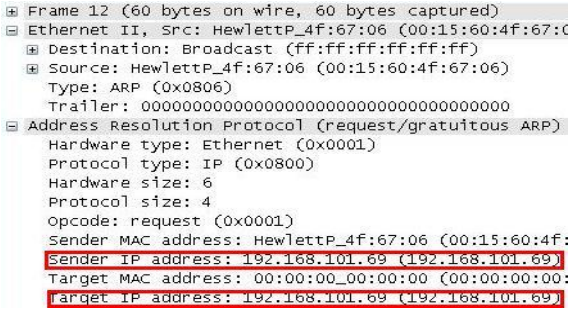
圖五、佈建偽裝偵測系統建構演算法

(1) 偵測點系統首先先發 TTL=1 封包尋找 Default Gateway。

(2) 有了 Default Gateway 之後，即可發送 ARP Request，將 Default Gateway 設為做後一個詢問點，當 Default Gateway 回復及代表存活表已建立好。

(3) 判別封包目的雲端 IP 是否存活，如沒有則發出偽裝封包保護雲端區網。一般而言，當雲端網內主機起動時，會先發送 Gratuitous Arp 確認欲使用的 IP 是否已被雲端網內的主機佔據，因此本系統會進一步檢查是否有後來才開機的主機所發送的 Gratuitous Arp(如圖六)，如接收到的 IP 已被偽裝，則釋放此 IP，以利正常主機使用此 IP。Gratuitous Arp 的特性在 windows7 以前是 Source IP 跟 Target IP 相同，而在 windows 7 以後微軟將 Gratuitous Arp 改為 Source IP 跟 Target IP 皆為 0。

3.2.2 虛擬主機偵測點的釋放



圖六、Gratuitous ARP

```
while(true){
封包接收
if(封包!=null){
  if(封包類型為 ARPRequest){
    if(目標 IP 與來源 IP 相同&&IP 為偵測點||
目標 IP 與來源 IP 全為 0){
      從偵測點中釋放其 IP，將其 IP 加到存在
      IP 列表中;}
}  }  }
```

圖七、偵測點釋放建構演算法

3.2.3 偽裝偵測系統實驗結果

如圖八(顯示於參考文獻後)，外部使用者 210.60.168.125 訪問雲端主機 203.64.178.100，而 203.64.178.100 是不存在主機的 IP，子系統尚未運作時，訪問是沒有回應的(如圖八①)；本子系統會將其設為偵測點(如圖八②)，當其被訪問時，此子系統會替其進行偽裝且與外部 IP 訪問者進行互動(如圖八③)。由於 203.64.178.100 是不存在之主機的 IP，但卻有外部的 IP 進行訪問，其可能是攻擊者的機率頗高，所以將此外部 IP 寫入嫌疑表(如圖八④)，並告知其他地域的子系統。

3.3 弱點偵測系統

雲端主機如遭受到入侵，不僅資料嚴重的外洩，還有可能會被當作攻擊雲端服務主機的跳板，而通常入侵者能入侵雲端的主機，都是透過雲端主機作業系統的漏洞。弱點偵測系統依據分流偵測系統記錄曾經被攻擊的高風險主機做作業系統現有的漏洞分析，其有一套漏洞解決方案的資料庫，經過比對之後，能對有漏洞的主機提供最完善的補強方案，並提供給管理者，減少雲端主機被入侵的機會。

如圖九(顯示於參考文獻後)為使用 Nessus 針對 TCP 80port 所做的 PHP 版本弱點分析；此問題為 PHP 版本過舊，舊版本的$GLOBALS 全域變數可以遭到漏洞所修改；解決方法為升級至 PHP 版本 4..4.1/5.0.6 以上即可解決此漏洞。弱點偵測系統會根據漏洞報告彙整問題、問題敘述以及解決方法，彙整後系統會自動發訊息給管理者，管理者便可透過此訊息，對弱

點主機進行漏洞處理，如此能進一步避免雲端伺服器在網際網路上所受到入侵攻擊。

3.4 協同合作系統

協同合作系統的產生，是由於傳統的入侵偵測系統利用攻擊行為特徵，逐一比對每一筆封包，當有巨量的攻擊發生時，比對封包的時間可能以指數成長，而無法即時有效的抵擋攻擊，因此協同合作系統利用網際網路分散式的特性，雲端中的各入侵偵測系統互相合作，交換攻擊者的資訊(如圖十，顯示於參考文獻後)，如此可以分散單一入侵偵測系統比對的時間，更可以即早的抵禦雲端外部的攻擊者。

當協同合作系統收到來自於偽裝偵測系統的訊息(如圖十①)，系統會將嫌疑 IP 告知分流偵測系統和其他跨地域協同合作系統；當收到來自於分流偵測系統的訊息(如圖十②)，系統會將需阻擋 IP 告知其他跨地域協同合作系統，進行 IP 阻擋；當收到來自於其他跨地域協同合作系統的訊息(如圖十③、④)，系統會將嫌疑 IP 或需阻擋的 IP 寫入嫌疑表和阻擋表，並告知分流偵測系統進行阻擋。如圖十二為本研究之四個子系統相互合作的通訊協定。

4. 結論

本研究的系統建構在四個子系統運行的合作上，當雲端其中一個地域雲遭受到了攻擊，其他坐落於不同地域的雲則會收到警報的訊息，即時的抵禦攻擊者，減少單一入侵偵測系統分析封包的時間，提升找出攻擊者的效率。本系統也 m 能將曾遭受到攻擊的高風險 IP 進行作業系統漏洞的補強，減低被入侵的機會。除此之外，本系統也在雲端建置了多重偵測點，當攻擊者和不存在主機的 IP 溝通時，能替其進行回復，讓攻擊者誤認為其是個可攻擊的對象，如攻擊者進行攻擊，並不會真的損害到實體的主機，還能即早的偵測出潛在的入侵攻擊者，經過實際建置並運用於聯大資管系的網路中，證明其具備相當程度的可行性。

5. 參考文獻

[1] ”趨勢：Google 遭攻擊，凸顯雲端安全重要性”,http://www.zdnet.com.tw/news/software/0,2000085678,20143834,00.htm

[2] ”IBM WebSphere Application and Business Integration”,http://www.nti.com.tw/wbi.htm

[3] “Disk Array”, http://zh.wikipedia.org/wiki/%E7%A3%81%E7%9B%98%E9%98%B5%E5%88%97

[4] A Platform Computing Whitepaper, ‘Enterprise Cloud Computing:Transforming IT’, Platform Computing, pp6, viewed 13 March 2010.

[5] Dooley B, 2010, ‘Architectural Requirements Of The Hybrid Cloud’,Information Management Online, viewed 10 February 2010, from <http://www.information-management.com/news/hybrid-cloudarchitectural-requirements-10017152-1.html>

[6] Global Netoptex Incorporated , 2009, Demystifying the cloud. Important opportunities, crucial choices, http://www.gni.com, pp 4-14, viewed 13 December 2009.

[7] Lofstrand M, ‘The VeriScale Architecture: Elasticity and Efficiency for Private Clouds”, Sun Microsystems, Sun BluePrint, Online, Part No 821-0248-11, Revision 1.1, 09/22/09

[8] Ramgovind, S.; Eloff, M.M.; Smith, E.,“The management of security in Cloud computing”

[9] “VMware Workstation”,http://andyshyu.blogspot.com/2009/07/vmware-workstation.html

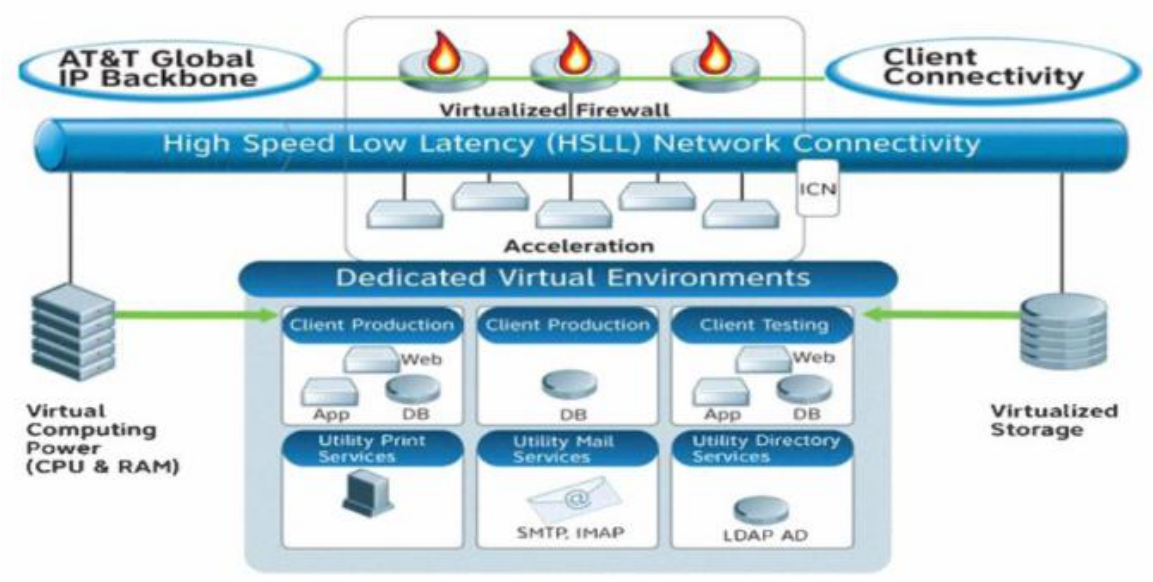
[10] “VMware DRS”, http://software.bestcom.com.tw/down/dwon_file.aspx? file=20080311102921Y35GQ. pdf&filetype=9&DC_ID=9

[11] “VMware Fault Tolerance”,http://www.zerone.com.tw/support/VMware/VMwareSiteRecoveryManager.pdf

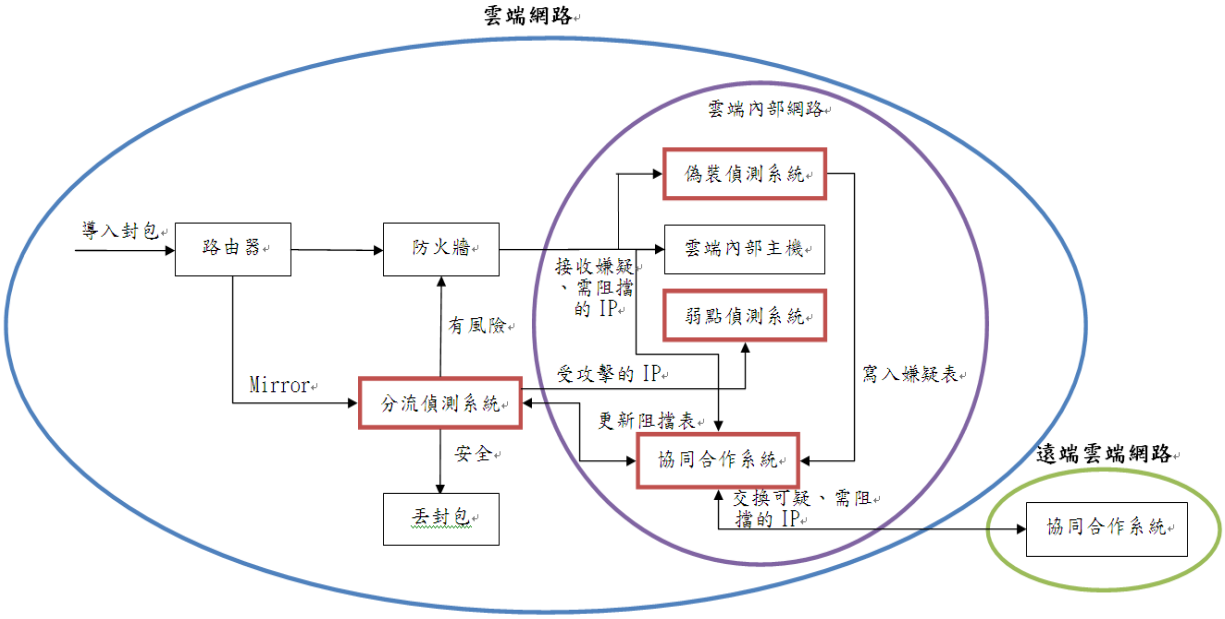
[12] Almulla, S.A.; Chan Yeob Yeun; ‘Cloud computing security management’

[13] Lejiang Guo; Fangxin Chen; Li Chen; Xiao Tang; ’The building of cloud computing environment for e-healt

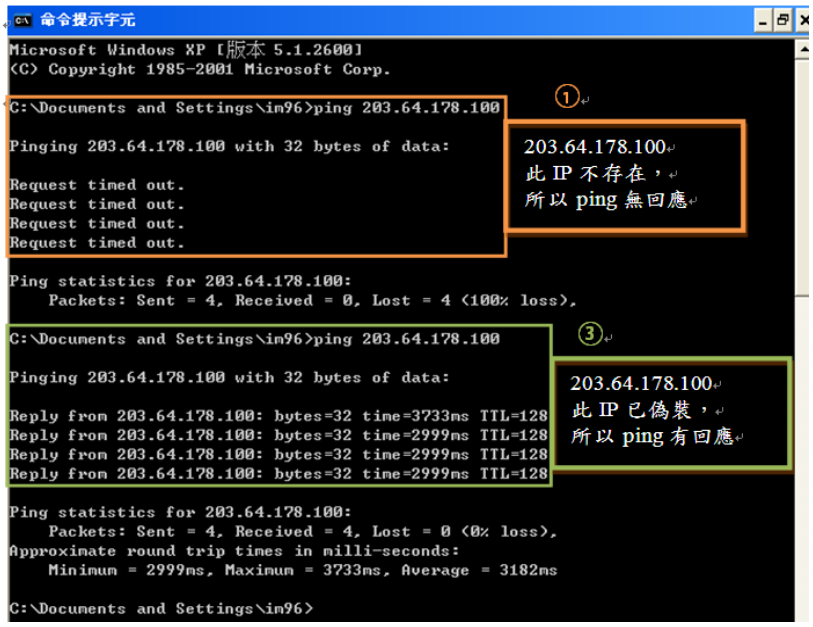
h’
[14] Chi-Chun Lo, Chun-Chieh Huang, Jo y Ku, "A Cooperative Intrusion Dete ction System Framework for Cloud Computing Networks," icppw, pp.280 -284, 2010 39th International Confere nce on Parallel Processing Workshop s, 2010
[15] D.J. Ragsdale, C.A. Carver, Jr. J.W. Humphries, U.W. Pooch,“Adaptation techniques for intrusion detection an d intrusion response systems,” 2000 I EEE International Conference on Syst ems, Man, and Cybernetics, Vol.4 , 8-11 Oct. 2000 p.2344-p.2349.
[16] E.H, Spafford and D. Zamboni, “ Intrusion Detection Using Autonomo us Agent,” Computer Networks, vol.3 4, issue 4, 2000,pp.547-570.
[17] S. Cheung, R. Crawford, and M. Dil ger et al., “The Design of GrIDS:A Graph-Based Intrusion Detection Syst em,” Technical Report CSE-99-2, U. C. Davis Computer Science Departm ent, January 1999.
[18] S.R. Snapp, J. Brentano, G.V. Dias, T.L. Goan, T. Grance, L.T. Heberlein, C.L. Ho, K.N. Levitt, B. Mukherjee, D.L. Ma nsur, K.L. Pon, and S.E. Smaha, “A syst em for distributed intrusion detection,” Co mpcon Spring’91, Feb-March 1991, pp.17 0-176.



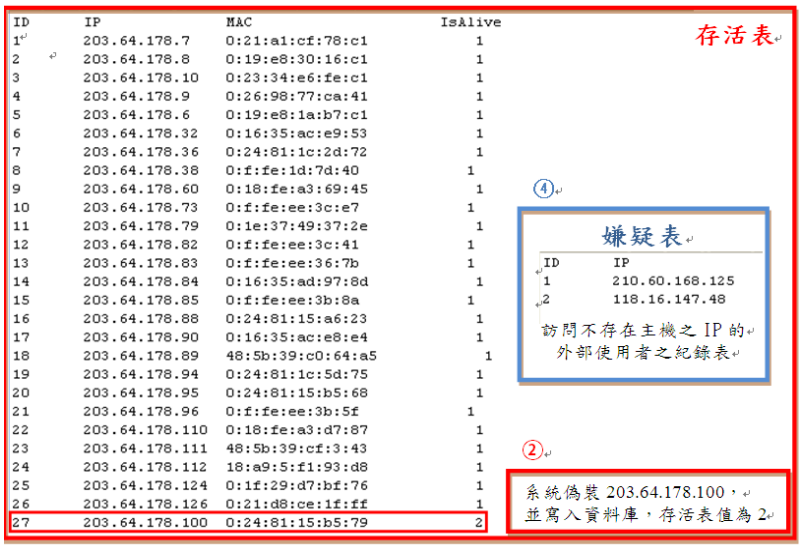
圖二、HFMS 架構圖



圖三、雲端攻擊偵測系統架構圖



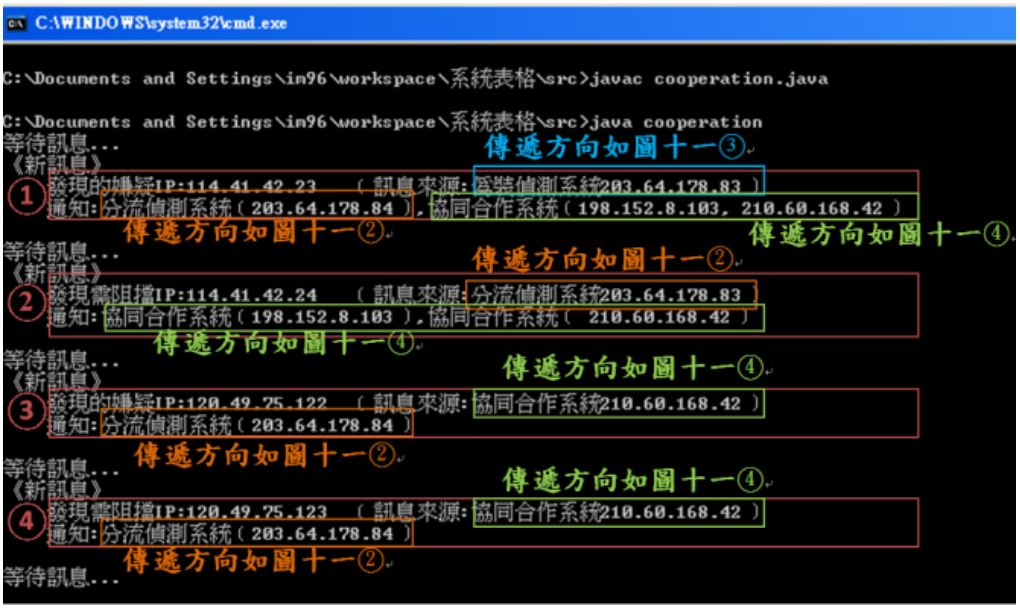
外部使用者(210.60.168.125)



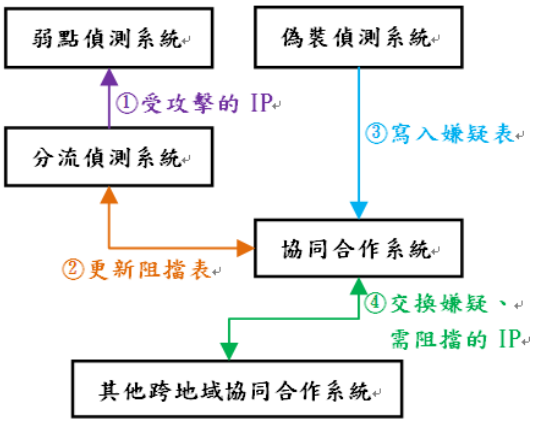
偽裝偵測系統(203.64.178.100)

圖八、偽裝偵測系統運作圖

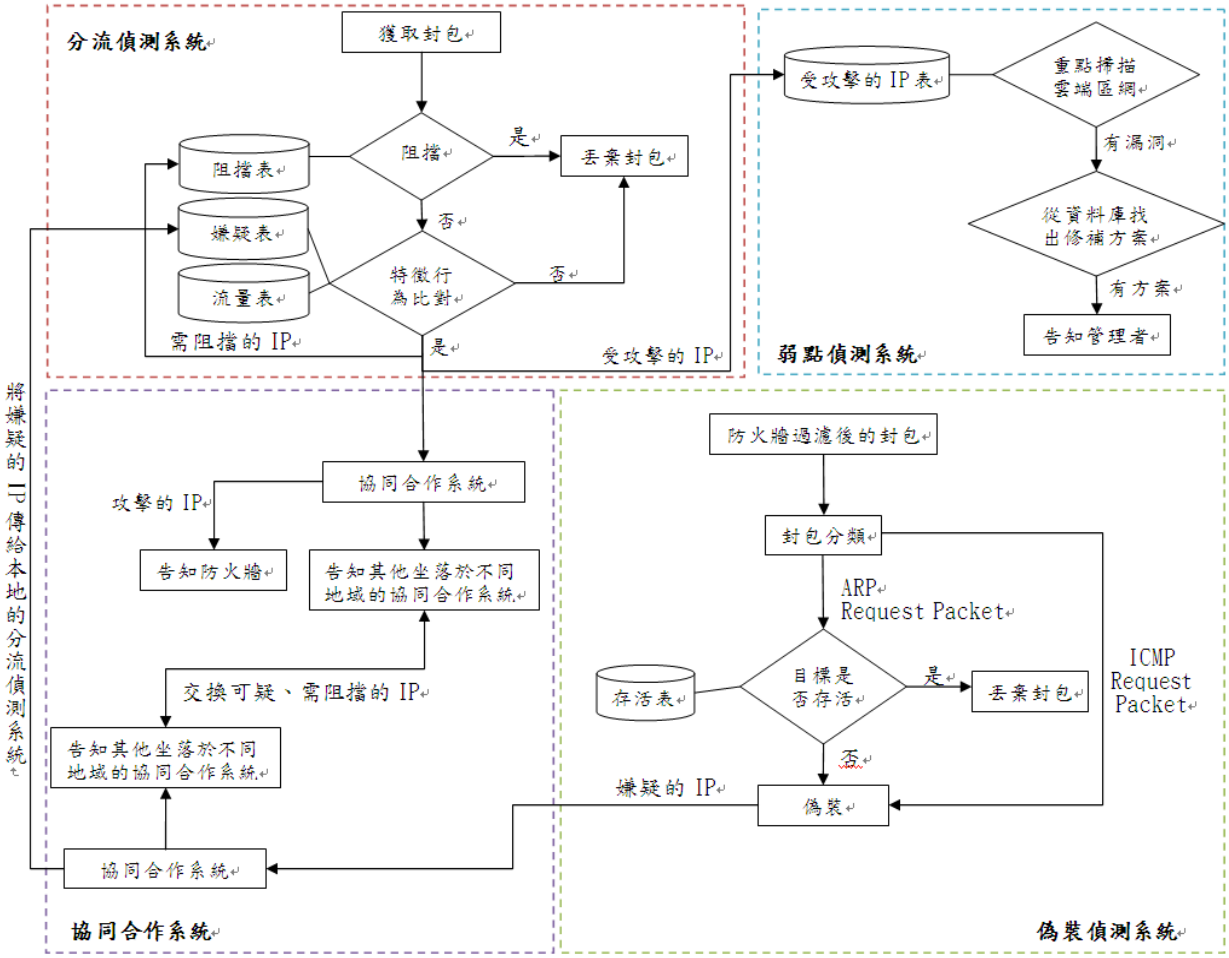
圖九、Nessus漏洞報告



圖十、協同合作系統模擬結果



圖十一、訊息傳遞路徑圖



圖十二、系統流程圖