出國報告（出國類別：國際會議）

第六屆遺傳與進化計算國際會議
The Sixth International Conference on Genetic and Evolutionary Computing

服務機關：中興大學資訊管理系
姓名職稱：林詠章 教授
派赴國家：日本 北九州
出國期間：2012/8/25-2012/8/28
報告日期：2012/11/15

摘要

第六屆 International Conference on Genetic and Evolutionary Computing 今年暑假在日本北九州的小倉舉辦，會議地點在北九州會展中心，會議中有許多國內外學者參加共團探討資訊科技的最新發展，而本人最近所投入的雲端技術也是此會議的重點研究領域之一，也是目前非常熱門的研究範疇，在此會議中也有多位學者發表雲端技術的相關論文。除此之外，在此次會議中，我們也發表一篇名為“A Cloud-user Access Control Mechanism based on Data Masking”之論文，該論文主要是針對雲端使用者所存放於雲端儲存空間所做的一些保護，而在保護機制中使用者鑑別(User Authentication)及存取控制(Access Control)機制，此技術可以說是雲端保護最前線的兩到防禦關卡，在會議中也與許多學者針對此一議題有廣泛的討論，獲益良多。此研究議題亦符合目前著重於雲端科技安全及個人資料保護機制的研究議題。

目次

一、 目的……4

二、 過程……4

三、 心得及建議…… ……9

四、 與會照片…… ……11

一、 目的

第六屆遺傳與進化計算國際會議(The Sixth International Conference on Genetic and Evolutionary Computing)，是資訊科技領域每年會固定舉辦的幾個重要研討會之一，亦是資訊科學與工程領域頗具知名度的學術會議，會議論文集亦收錄於 EI Index，今年本人有一篇研究論文投稿至此會議，很榮幸被接受並發表，這篇論文名稱為"A Cloud-user Access Control Mechanism based on Data Masking"，這篇論文主要對雲端服務的使用者作一些存取控制的安全保護，不同於傳統的存取控制技術，在雲端的環境裡，使用者擔心的是我們把資料放在雲端裡安不安全，雲端服務的提供者會不會監守自盜竊取我們放在雲端上的資料。因此，雲端安全已是雲端服務能不能持續發展最重要的原因之一了，如何讓使用者能安心將資料放在雲端儲存空間上就是一個很重要的課題。我們想透過這一次的研討會，將我們最新的雲端存取控制技術作一個介紹，希望透過這次會議的平台，能獲得國內外專家的一些建議與指教，讓我們所研發的這個技術能更加成熟。此外，這個會議亦規劃了幾個很重要的議題，比如說影像應用、資訊隱藏等等，我們也希望透過參加此次會議的機會，多瞭解一下目前世界各地學者所做的研究方向，彼此交流研究經驗。

二、 過程

The Sixth International Conference on Genetic and Evolutionary Computing 今年（2012 年）8 月 25 日在日本北九州召開，這次會議由 IEEE, 日本的 IEEE, The Waseda University 及台灣的高雄應用科技大學所共同舉辦，該會議至今已經進入到第六屆了，是資訊科學與工程相關研究之重要會議，這次會議主辦單位選擇在離福岡不遠的小倉舉辦，會議地點的北九州會展中心是一棟很新穎的建築物，戶外的公共空間很寬闊，會場內動線也規劃良好，會議的地點離小倉的 JR 車站也不遠，步行 10 分鐘即可到達，十分方便。

本次會議主要提供了一個讓專家學者深入探討資訊科學、工程及通訊技術學理

發展與經驗交流之機會。會議主題包含四個 Track，其內容如下：

Track I: 基因運算(Genetic Computing)

- 基因運算及演算法
- 生成和發展系統
- 基於遺傳學的機器學習與學習型分類系統 s
- 遺傳編程的性能和行為的實證研究
- 混合體系結構，包括遺傳編程組件

Track II: 進化計算(Evolutionary Computing)

- 進化的設計與應用
- 進化樹或圖形結構
- 不同類別的自動機或機器的進化
- 進化的組合和多目標優化
- 進化策略，進化規劃
- 進化調度和路由
- 生物資訊和計算生物學

Track III: 智慧運算(Intelligent Computing)

- 群智能優化
- 蟻群優化和群智能人工免疫系統
- 人工智慧與決策支援系統
- 智能資訊融合和資料探勘
- 智慧資料庫系統
- 知識發掘與管理
- 類神經網路及其應用
- 模式識別和自適應技術
- 智能計算機視覺和科學可視化

Track IV: 網格計算(Grid Computing)

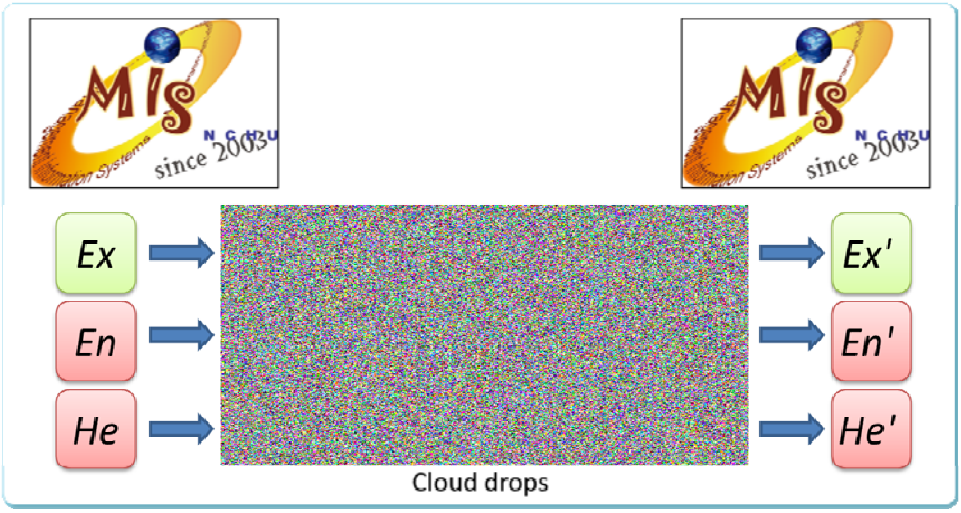
- 網格資源管理與任務調度
- 網格信任和安全
- 分散式平行計算
- 分散式智能處理

這些領域都是目前資訊科技極重要的幾個發展方向，這次參與會議的學者以台灣、日本、韓國居多，大家參與熱烈，幾乎很少有學者沒有來發表論文。

在這次會議中，所有被接受發表的論文都是經過兩位以上審查者嚴密的論文審查過程之後才接受發表，此次會議的論文集亦被 EI 收錄並出版會議論文集。在這次會議中我們研究團隊有一篇論文被接受發表，這篇論文題目為“A Cloud-user Access Control Mechanism based on Data Masking”， 其內容是說明雲端應用的發展中所提供的儲存空間及分享平台，使用者將數位資料儲存於雲端平台中，檔案受到平台的存取控制機制所保護，避免其他人非法使用這些數位檔案。但若雲端平台受到入侵，攻擊者可不經過平台的驗證機制，進入平台的主機直接取得這些數位檔案。這會使數位檔案暴露在不安全的雲端環境之中。我們所發表的這篇論文即是針對這樣的問題，提出一個基於資料遮罩(Data Masking)的存取控制機制。利用使用者驗證資訊置換數位檔案位元資料，使數位檔案因位元資料不正確而無法被正確且完整的開啟。合法使用者利用正確的驗證資訊可還原數位檔案被破壞的部分，避免數位檔案被非法存取以及濫用，讓使用者可以更放心的使用雲端資源所帶來的便利。

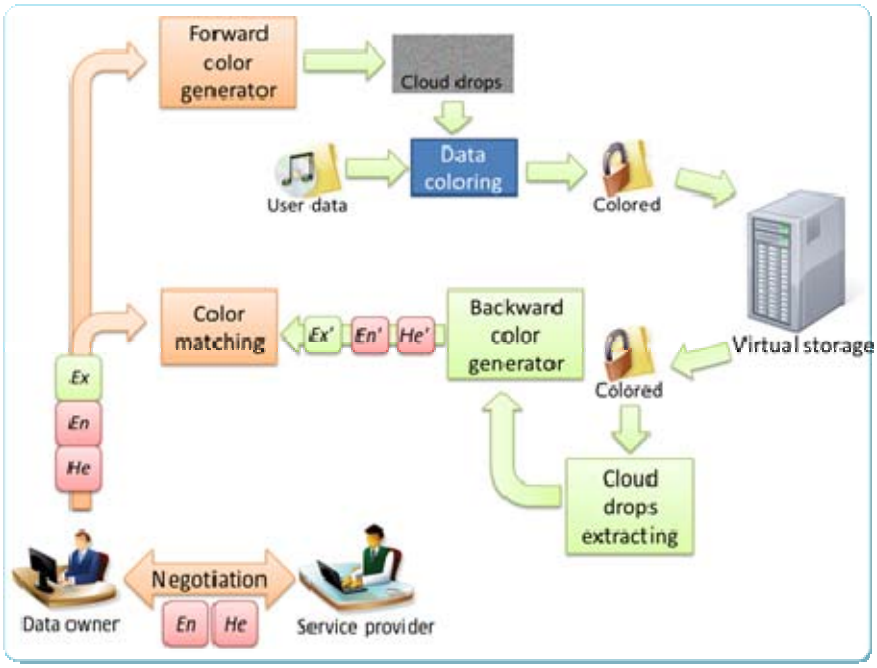
在我們所提出的技術中，我們是希望能透過「雲滴」(Cloud Drops)的概念，如下圖，為資料上色，作為檔案擁有者的標示。在一個雲端服務平台中，使用者要將一份檔案傳送處存置雲端儲存空間中。假設雲端服務提供者是可信任的，而資訊傳送是在一個安全的環境中進行。使用者利用函數取得這份檔案的特徵值(Ex)，並與服務提供者協議出的兩個亂數值(En)與(He)，目的用來增加雲滴的亂度。利用這三個值產生出雲滴影像，並用浮水印技術將影像嵌入檔案之中，完成資料的上色，再將上色

後的資料存入雲端儲存空間中。當使用者要求取得這份檔案時，系統取得嵌入檔案中的雲滴影像，並還原三個值(Ex')、(En')以及(He')，在與使用者所輸入的(Ex)、(En)與(He)驗證無誤後，才將檔案傳送給使用者。



下圖是整個機制的運作流程，我們應用雲滴的概念，提出了一個基於資料遮罩(Data Masking)的保護機制來保護使用者存放於雲端儲存空間的資料。檔案擁有者設定一個亂數種子，並透過亂數種子來產生出一組亂數序列。依照每個序列的值來提取檔案資料對應位置的位元值，將取出來的位元值與擁有者所擁有的秘密值做輕量的加密計算。當使用者取得受到保護的檔案，並要將檔案解密時，需利用原本所設定的種子來取得的原始的亂數序列，再透過亂數序列以及使用者的秘密值來還原加密過的位元值。若無法還原正確的序位元值，檔案內容將毀損或無法正確的開啟。

在安全性分析方面，我們的方法是將經過資料遮罩後的檔案資料傳送到雲端平台中。該份檔案資料的位元資料經過遮罩的計算破壞，造成檔案結構以及其中所包含的資料與原本之檔案資料有相當之差異。當檔案結構或資料受到破壞時，應用程式將無法開啟結構受到破壞之檔案。因此，當攻擊者透過伺服器入侵攻擊或內部存取攻擊來取得檔案資料時，無法正確地取得完整的檔案資料內容。



在資料遮罩的攔截與猜測攻擊上，我們的方法在資料傳輸的過程中，並不會傳送產生資料遮罩的參數。當攻擊者攔截使用者每份受到資料遮罩保護的資料並無法猜測或歸納出資料遮罩之資訊。因為每份檔案資料所使用的資料遮罩皆是獨立相關於該份檔案。

在暴力攻擊方面，去除資料遮罩的過程中，攻擊者無法透過暴力破解的方式來去除遮罩。資料遮罩的計算使得檔案資料的位元值受到計算破壞，但在計算的過程中，並無特定的規則來針對特定的位元資料來計算，因此沒有規則可循。以檔案大小在 1M 以上的檔案來分析，透過暴力破解來計算檔案資料的每個位元值，需要計算 2^{28} 個位元值。當檔案大小越大時，計算量會更多。當攻擊者能成功利用應用程式開啟檔案時，無法確定檔案內容與原始檔案相符合，因此無法判定攻擊是否成功。

資料遮罩的機制提供給使用者選擇遮罩長度，透過隨機選擇位元值計算的方式來完成資料遮罩。透過部分破壞的方式使得檔案資料無法正確的被開啟。但若是攻擊者分析檔案位元的片段資料，則有機會取得檔案資料的部分片段內容。因此，若要放置於雲端平台中的檔案資料是機密資料，則使用者必須選擇與檔案長度相同的遮罩長度，才可達到安全的保護。

現在普遍所使用的行動運算裝置如：智慧型手機、平板電腦、筆記型電腦等，在電力支援與運算能力已有相當程度的提升。智慧型手機與平板電腦的運算核心在 2011 達到 1GHz 雙核心的規格。筆記型電腦除了運算核心達到四核心的運算效能外，在電力續航力的支援也達到 6 小時以上。資料遮罩所使用的是輕量的計算保護，不會造成現今普遍使用之行動專制的效能負擔

整合上述的想法，後續我們應可將此技術做一個延伸應用，擴展到更多的應用領域。

本人這次行程也順道參加相關的演講活動，該會議也包含了數個不同議題的研討會，與會學者相當多，也與許多來自不同國家的學者進行相關研究問題的交流與經驗的分享。例如，來自台灣亞洲大學的周教授所發表的在 HTML 檔案上的可回覆式資訊隱藏技術(A Reversible Data Hiding Scheme Using Cartesian Product for HTML File)其研究就非常值得我們團對參考，一般文字檔案很難藏入資訊，但他們利用 HTML 檔案的特性巧妙的的將機密資訊藏入,且將機密資訊取出後又不會破壞原始的 HTML 檔案，這是一個非常有創意的應用。另外，靜宜大學得林教授也發表一篇可回覆式的資訊隱藏技術(A Reversible Data Hiding Scheme for Block Truncation Compressions based on Histogram Modification)，其最大的特色是可利用影像壓縮的概念來將機密資料藏入，且取出資料後可使原始影像不失真，這些技術對我們後續的研究具有很高的參考價值。

三、 心得及建議

The Sixth International Conference on Genetic and Evolutionary Computing，會議流程及提供的服務良好，其環境幽雅，會場動線規劃良好，讓與會專家學者留下極為良好的深刻印象。此外，這次會議的晚宴極為特別，是在一飯店的高樓層舉辦，與會者都是站著用餐，這樣的用意可能是希望大家能互相交流，而不是指跟同一桌的人有互動而已，而事實證明這樣的效果也的確不錯，大夥熱烈的聊天討論，這樣的方

式也可提供給後續要辦研討會的舉辦者一個參考。

在我的研究範疇上，雲端服務也是大家熱烈討論的議題之一，我發表完我的論文後，也有學者前來討論交流，得到的共識是現今雲端應用的發展提供使用者一個線上資料處理的平台，安全與否是雲端發展能否成功的關鍵要素，在這平台之中，使用者將檔案資料存放於雲端儲存空間，透過服務提供者所提供之雲端服務來處理這些檔案資料。而我們的研究提出了一個基於資料遮罩的存取控制機制來增進雲端平台對於使用者資料的保護，利用資料遮罩之計算，檔案資料的原始位元值受到計算修改，使得檔案結構與內容受到破壞。當雲端平台受到攻擊導致檔案資料被竊取時，攻擊者無法取得正確之資料內容。此外，輕量化的運算機制使資料遮罩階段與去除遮罩階段能於使用者所擁有之一般裝置或行動裝置上執行。因而無須傳送執行資料遮罩所使用之驗證資訊，降低驗證資訊外洩之風險，提升雲端服務之安全性，進而提高使用者對於雲端平台之信任度，讓使用者能更放心地使用雲端服務所帶來之便利。也藉由此次會議拋磚引玉，期望有更多學者能投入此一研究領域，政府及產業也能多重視雲端資訊安全的發展。

四、　　與會照片

會議舉辦地點-北九州會展中心 新穎的外觀

學者發表論文情形