

出國報告（出國類別：參加國際研討會）

## 2013 創新科技&工業管理國際研討會

服務機關：國立中正大學資管系

姓名職稱：古政元教授

派赴國家：泰國

出國期間：102 年 05 月 27 日至 102 年 06 月 01 日

報告日期：102 年 06 月 14 日

## 摘要

此行的目的在透過參加相關的國際研討會，與國際學者互動討論並聽取各界學者的建議，以期能夠增加本研究計畫成果的完備性，藉以提供國內產官學研界做參考。在未來雛型系統開發及分析結果數據完備之後，我們還預計將最終版本提交到國際著名的學術期刊上發表。

整個研討會過程本人多有參與。5 月 29 日當天早上，我直接前往會場出席聽取各場次的 keynote speech，下午的第一場次則是我本人的報告，我在會場簡報並與眾學者討論得到了兩個重要建議：(1) 建立制度讓公正第三者的資料生命週期稽核報告可以有跟會計師簽證一樣的公信力；(2) 公正的第三者嵌入監控代理人的軟體以進行稽核的過程，最好納入雲端安全聯盟 (Cloud Security Alliance) 所提供的 CCSK (Certificate of Cloud Security Knowledge) 認證規範當中。5 月 30 日的最大收穫是認識了一位從波蘭來的副教授，他的名字是 Seweryn Spalek，目前在 Silesian University of Technology 任教，我們討論了很多問題，我打算邀請他在不久的將來前往台灣訪問我的學校，或者是客座一個學期。

重要的成果則是出席本研討會的學者對我們所提出的運作架構認為殆無疑義，只是後續的發展或延伸研究上有兩個如前所述的建議。這個初步發展看起來是相當不錯的，我們論文的最終完整版本會在雛型系統開發及分析結果附加上去之後投稿，上述一些學者所提供的很好建議我們會放在未來研究的章節裏，這對其他欲進行這方面研究的先進們應該有所助益，也會讓本文的內容更為完整全面，相信這也是參加這個國際學術會議最重大的收益。

# 目次

目的	4
過程	8
心得及建議	13
附錄一 參與研討會照片	15
附錄二 報告投影片	16
附錄三 研討會論文目次	20
附錄四 研討會論文	21

# 目的

## I. 計畫目標

本計畫欲達成的目標如下：

- (1) 提出一種有效的覆蓋機制來處理在雲端運算中資料殘留問題。
- (2) 提出一個基於雲端資料生命週期的安全處理機制。
- (3) 透過參加相關的國際研討會，與國際學者互動討論，期能夠增加本成果的完備性，藉以提供國內產官學研界做參考。

## II. 主題

當政府和企業專注於雲端運算的發展時，潛在的資訊安全問題浮出水面，此外，不同種類的雲端服務會面臨不同的安全性問題。新興的雲端計算技術需要能夠保證各種安全上要求，否則大多數的客戶組織將不敢採用它，在諸多的雲端服務資訊問題當中，資料殘留是一個最關鍵性的安全問題，因此本研究的主題即聚焦在提出了一個基礎架構來解決雲端中的資料殘留狀況。此外，縱然雲端服務提供商承諾資料的徹底清除，但這些過程是否有所保證？

綜而言之，本研究的主題將集中在解決以下兩點現況：

- (1) 目前雲端資料的殘留問題似尚未有具體的解決方法被提出。
- (2) 目前尚缺乏一種機制用於監測雲端資料的徹底清除。

## III. 緣起

近年來，隨著雲端運算變得越來越流行，它已逐漸引起政府和企業的重視。事實上，從另一個層面來看，促成雲端運算快速發展的一個重要因素就是前幾年的金融海嘯所導致的經濟衰退，由於經濟不振和成本效益的考量，企業必須找到方法來降低經營的成本與提升效益。從資訊科技的角度而言，雲端運算的出現提供企業一個機會，可以不用將心力分散在 ICT 基礎設施的管理，進而全心集中在核心業務上，因此能專注在提升自己的競爭力。

雲端運算的好處包括集中控制資源，降低軟硬體的成本，提供使用量計算費率，並減少人力資源的成本。根據美國國家標準與技術局（NIST）的定義，雲端運算供應商所提供的服務有三種基本模型式：

- 軟體即服務（Software as a Service, SaaS）：由雲端服務提供商提供軟體應用程序給客戶從遠端登入連線使用。用戶可以依需求在任何時間使用各式各樣的軟體，他們並不需要另行單獨安裝。
- 平台即服務（Platform as a Service, PaaS）：該服務為開發人員提供創建軟體應用所需要的平台。在雲端服務提供商的平台上開發人員可以編寫所需的軟體，用戶可以專注於應用程序開發，隨時部署自己的基礎環境，包括開發系統，網路或儲存設備，因此可以降低設備和管理的成本。
- 基礎設施即服務（Infrastructure as a Service, IaaS）：其目標是提供一個有彈性的且符合標準的基礎設施環境，讓使用者可以建立 PaaS 和 SaaS 的服務。

當政府和企業專注於雲端運算的發展時，潛在的資訊安全問題浮出水面，此外，不同種類的雲端服務會面臨不同的安全性問題。隨著這些年台灣的經濟迅速增長，許多企業和機構產生了大量的用戶資料。這些資料通常足以直接或間接識別一個人的身份，包括：

個人訊息，如姓名，性別，年齡，出生日期，地址等。

具體訊息，如婚姻狀況，電話號碼，帳號，健康情況，生活習慣，私人照片等。

透過資訊傳輸和處理過程中的漏失，計劃收集用戶資料的惡意駭客更容易取得他(她)們想要的資料，有鑑於此，政府和企業或非營利組織應設法保護個人資料隱私。台灣個人資料保護法（PDPA）自 2012 年 10 月 1 日起生效，根據該法律的要求，政府機構和非政府組織都將受到 PDPA 的規範。幾個重要的條例概述如下：

- （1）當收集，處理或使用個人資料時，必須遵守法定要求和程序。
- （2）如果未能遵守 PDPA 的規範並且被指控而無法證明善盡管理者的責任時，將受到民事賠償的處

罰，每一事件最高可達新台幣 2 億元。

(3) 政府機構和非政府組織必須向法院證明，他們已經採取足夠的措施保護個人資料，資料的擁有者並不需要提供證據始可控訴。

上述的 PDPA 規定廣泛和顯著的影響所有企業和機構，所以他們應當採取必要的措施，包括正確的合約規則，政策及措施等以符合 PDPA。

本計畫的研究標的即著眼在影響個資安全最大的資料殘留問題，當使用者在一台個人電腦上刪除文件，他(她)將拖拉文件到垃圾桶，然後清空資料回收站。大多數人其實並不知道，實際上他(她)並沒有刪除文件，只是文件系統中的文件路徑被刪除掉而已。事實上，該文件仍然留存在硬碟上，直到下一個新文件儲存在相同的位置加以覆蓋為止。我們稱這個問題為資料殘留，在雲端上，資料殘留的問題將會更為複雜且不易處理解決。

誠如前述所言，資料保護已經成為一個非常重要的議題。根據個人資料保護法，企業被要求在使用個人資料時，必須善盡管理人的保護責任。如果企業故意或無意洩露個人資料的話，他們將被罰款以彌補客戶的損失。當企業使用雲端運算以增強其競爭優勢時，他們需要尋找可靠的解決方案來保護他們的業務資料。在某些情況下，客戶或利益相關者懷疑企業資料保護的努力時，企業或組織有需要提供有力的資料保護報告，以證明客戶的資料得到了適當的保護。為了達到雲端客戶的信賴，雲端資料需要有一個公正第三者 (Trusted Third Party, TTP) 來監控其整個生命週期的安全，這就如同會計師提供審計過的財務資料一般。我們提出的機制將代理監測數據在使用雲端計算時的整個生命週期，並確保數據在不使用時可以徹底清除。這個機制可以根據客戶的要求提供一份審計報告，基於這樣的設計，我們嘗試解決雲端服務中用戶最在意的數據清除問題，這也是一個最關鍵的安全問題。我們設計的主要優點是，客戶不需要改變他們原來使用網路的習慣，也就是說，這個安全操作的機制對最終用戶而言是透明的。完整的基礎架構決定後，將完成計劃中所提之雛型系統，再進行安全性分析和效能分析。我們預計，這個機制應該可以符合用戶對雲端運算的安全性和性能要求。眾所周知，雲端計算的安全性符合要求後，才可以談管理和保障，而雲端計算服務的未來也方有前景可言。

#### IV. 預期效益及欲達成事項

本計畫預期在參加2013 創新科技&工業管理國際研討會時，可以和許多來自各國的學者一起討論，並且獲得他們寶貴的建議，藉以修訂我們所提出的新型基礎架構與機制，期能更加確保雲端運算中的資料安全，在爾後進行雛型系統開發，及至分析結果數據完備之後，未來我們還計畫將最終版本提交到國際著名的學術期刊上發表。

## 過程

到達 2013 年科技創新與產業管理國際會議 Conference on Technology Innovation and Industrial Management 的註冊報到現場後，我開始和一些也來註冊的知名外國學者交流做研究的經驗和意見，報到不久後，科技創新與產業管理國際會議 Conference on Technology Innovation and Industrial Management 在會場舉行開幕接待會，此時許多學者和我談得很投機，這時也有很多年輕的學生出席，事實上，這次和資深或新進學者交談討論我有不少的收穫，最主要是聽到不少學者有關如何促進與推動產業科技創新的做法與想法。

### I. 會議議程

本次會議的官方會議議程如下：

Tuesday, 28 May 2013	
18.00-19.30	Registration  Welcome reception: Dean from Faculty of Business Administration and Dean from Faculty of Engineering, Kasetsart University
Wednesday, 29 May 2013	
8.00-9.30	Registration
9.30-10.10	Conference opening by hosting universities  Deputy Provincial Governor, Phuket (Dr. Sommai Prijasilpa)  Dean, Faculty of Engineering, Kasetsart University  Dean, Faculty of Business Administration, Kasetsart University (Dr. Bordin Rassameethes)  Welcoming address by TIIM Honorable Executive Committee (based on the previous hosting universities)  Dr. Binshan Lin, Louisiana State University in Shreveport, USA  Dr. Pekka Kess, Oulu University, Finland  Prof. Ryszard Debicki, Vice Rector for Science and International Cooperation,



	Maria Curie-Sklodowska University in Lublin, Poland
10.10-10.40	Keynote speaker: Mr. Marc Spiegel President: Thai-Finnish Chamber of Commerce Presentation scope: Globalization implications on business and industrial development: Asian experiences
10.40-11.00	Morning break
11.00-11.30	Keynote speaker: Dr. Kongkiat Kespechara Managing Director: International Medical Software and Software Park Phuket Deputy CEO-Bangkok Southern Hospital Group Presentation scope: Developing and managing Thailand's first privately-owned software park: lessons learned
11.30-12.00	Keynote speaker: Dr. Nitinai Sirismatthakarn Research fellow: Ministry of Finance (Thailand) Presentation scope: National KPIs reflecting the country's industrial competitiveness: Thailand and Southeast Asian region's experiences
12.00-13.30	Lunch with TIIM 2014 presentation (Seoul , South Korea)
13.30-15.30	Parallel sessions 20 minutes per paper
15.30-15.50	Afternoon break
15.50-17.30	Parallel sessions 20 minutes per paper
18.00	Evening program and dinner Phuket Fantasea ( <a href="http://www.phuket-fantasea.com/">www.phuket-fantasea.com/</a> )
<b>Thursday, 30 May 2013</b>	
9.30-10.40	Academic Leadership Forum Future education under the new economy
10.40-11.00	Morning break
11.00-12.00	Editors' Panel Publications in international journals: knowledge sharing
12.00-13.30	Lunch with TIIM 2014 presentation (Seoul, South Korea)

	Award Ceremony: Best Paper Best Research
13.30-15.30	Parallel sessions 20 minutes per paper
15.30-15.50	Afternoon break
15.50-17.30	Parallel sessions 20 minutes per paper
18.30	Evening program and dinner Farewell dinner
<b>Friday, 31 May 2013</b>	
9.30-12.00	Company Visit: Bangkok Hospital Phuket ( <a href="http://www.phukethospital.com">www.phukethospital.com</a> )

5月29日，我直接前往會場出席，清早的 keynote speech 是由一些知名的泰國官員和學者分別做數場報告，現場如附錄一圖一及圖二的照片所示，泰國官員的演講一直強調如何運用創新科技來推動產業的提昇，尤其是將套牢在產業界的諸多限制與枷鎖去除，以讓產業界有更大的自由空間可以大展身手，看到泰國官方如此積極進取，實在感慨我們要更加油了。

## II. 議場主題

大會的主題包括多種學科領域：會計資訊科技、品牌價值和管理、變更管理、企業融資、企業，運營和生產策略、文化多樣性、顧客心理、客戶關係管理、電子商務與電子商業、電子學習和人力資源、電子和行動政府、企業和營運風險、綠色技術和生產力、資訊管理與電腦安全、創新管理、國際業務及市場、投資、知識管理、管理及企業發展、管理資訊系統、營銷策略和管理、併購和收購、動機與情緒智慧、網路政府、新產品和服務開發、一站式服務、組織心理學、績效衡量與管理、電子商務中之隱私和安全問題、生產技術、管理和改善生產力、宣傳媒體、公共價值、品質改進和管理、社會營銷、供應商夥伴關係和供應鏈管理、持續經濟、經營和產業化經營技術、加值管理等。

我的演講定在 5 月 29 日下午 13:30 左右的場次 3 的第二個報告，這個場次的主題是：技術與創新管理 - 應用案例，新產品/服務的發展。

### III. 個人所發表內容摘要、現場報告或討論交流情形

我準時在 5 月 29 日下午 13:15 左右，也就是提早 15 抵達會場，雖然是第二個報告，但我早早就將 power point 上載妥當，本場次開始時所有六個報告人都出席，但因為第一個報告者的 power point 一直有問題而尚未搞定，場次主席 Victor Chen 詢問我這位第二個報告者可否先行報告，所以我就更動到本場次的一開始就進行演說，現場如附錄一圖三、圖四及圖五的照片所示。

我提出一個嶄新的基礎架構，它可以確保在雲端計算環境下，不使用的數據在客戶決定刪除他們時得以徹底清除。為了解決資料殘留問題，整個數據的生命週期都必須被監測，通過這種方式，我們可以詳細瞭解數據的使用和儲存的詳細過程。我們所設計的監控機制有三個主要的參與者，包括：資料擁有者、雲端運算服務提供者及公正的第三者。在雲端運算的環境中，客戶的資料會出現在虛擬機上的應用程序，平台或基礎設施裏，因此，我們的機制將透過公正的第三者在每一個 VM 主機應用程序及資料庫中嵌入監控代理人的軟體，它們會隨時回報雲端運算服務商處理、傳送與儲存顧客資料的詳細過程，公正的第三者再將這些資訊整理形成有公信力的正式監察或稽核報告。

聽眾們留下非常深刻的印象，除了讚許之外，他們還提供了很多有用的建議，讓我未來有改善的方向，他們並也表達了合作的意願。其中一個最重要的建議是，提醒我應當繼續聚焦於如何讓公正第三者的數據生命週期的監控報告可以有跟會計師簽證一樣的公信力，並且他們也特別強調這個議題將不再是技術問題，是如何建立報告的權威性和不可挑戰性，這是社會組織制度面的問題，事實上也是較實務面與心理層面的問題，但對產業界的貢獻將會更為明確。另外還有一名來自歐洲的學者提到，公正的第三者嵌入監控代理人的軟體以進行稽核的過程最好納入雲端安全聯盟 (Cloud Security Alliance) 所提供的 CCSK (Certificate of Cloud Security Knowledge) 認證規範當中，如此才較易取得國際使用者 (International users) 的信任，如果要納入雲端安全聯盟的規範則必須要有完整且鉅細靡遺的技術規格才有可能列入提案討論。當場我非常謝謝他們的建議，並且回答這將列入我未來的工作方向之一。

#### IV. 聽取報告議題之內容重點摘述、見聞或新知

在我參與的各個場次中，有一個報告者談到綠色供應鏈的發展越來越受歡迎，但大多數企業仍然不知從哪裡開始起頭。此外許多人仍然誤解綠色供應鏈不必然會改善效率和降低成本，但事實上現今綠色供應鏈強調兩個主要標竿並不與企業目標違背：

##### (1) 越來越多企業將綠色供應鏈管理的目標與業務目標看齊

建立綠色供應鏈並不必然會阻礙公司實現其業務目標。例如，如果一家公司決定使用可分解的包裝，但其比傳統的包裝多出成本 50% 以上，這顯然不符合其降低成本的業務目標，所以這時企業理當另選擇與業務目標相吻合的綠色供應鏈，並思考如何過渡到綠色供應鏈才可以幫助實現這些目標。也例如，如果一個企業要降低能源成本，它應該開始尋找並使用更節能，更環保的設備。

##### (2) 使用綠色供應鏈是改善企業流程的企機

通常公司並不輕易改變他們的業務流程，也就是這樣的態度讓企業流程的效率低下，造成不必要的浪費和污染的有增無減。要過渡到綠色供應鏈的企業應該藉此機會檢討所有的業務流程，檢討沿供應鏈的每個進程，以確定是否有更環保的方法有助於流程改善效率。

針對這些論述頗讓人對綠色供應鏈的看法有所更新。

另有一個報告者談到的官僚制度對科技創新與產業管理的制約，他旁徵博引的說明這個現象的存在與影響程度，這讓我的印象也非常深刻。

5 月 30 日的最大收穫是認識了一位來自波蘭的副教授，他的名字是 Seweryn Spalek，他目前在 Organisation and Management at the Silesian University of Technology 任教，他的專長非常廣泛，主要專注在 PM 與 MIS 相關的所有研究議題上，我們討論了很多問題，我打算邀請他在不久的將來前往台灣訪問我的學校，或者是客座一個學期。我在當天晚上找個機會再與 Prof. Seweryn Spalek 詳談，並一起合照留下記錄，如附錄一圖六的照片所示。

## 心得及建議

參與此次 2013 年科技創新與產業管理國際學術會議 Conference on Technology Innovation and Industrial Management，著實有不少的收穫，也讓我留下深深的印象。通過與來自世界各地的專家和學者討論交換觀點，我真的是得益於他們的嶄新看法。台灣的產業逐步走向全球化，網際網路和雲端計算也進一步加速許多企業的進步，但也讓我們面臨來自世界各地的強烈競爭。事實上，台灣的計算機和伺服器產業具有全球的領先地位，在世界上也成為許多國家的學習對象。但是，如果我們要更上一層樓，我們必須要特別注意雲端計算服務正在如何改變人們使用電腦和網路的行為。新興的雲端計算技術需要能夠保證各種安全上要求，否則大多數的客戶/組織將不敢採用它。我們的研究提出了一個基礎架構來解決安全的問題，亦即數據的徹底清除。眾所周知，雲端計算的安全性符合要求後，才可以談管理和保障，而雲端計算服務的未來也方有前景可言。由於台灣是最重要的數據及通信和網路產品的製造國，國內的許多網際網路服務商也計劃大力開發這方面的應用以增加需求。如果我們希望雲端計算能為我們的全球競爭力起到了重要作用，我們就必須設法提高世界各地潛在用戶對其安全上的信心。因此雲端計算和網際網路服務的未來發展需要投入許多資源在研究和開發的工作上，這包括軟體，硬體和資訊安全等議題。

我們提出的研究報告與雲端計算的資訊安全問題有關，實際上，它被認為是為未來雲端計算服務行業是否能成功發展的最重要因素之一。因此，這次演講吸引了很多目光焦點，我們確實也有一個相當熱烈的討論，所有的學者對我們所提出的運作架構認為殆無疑義，只是後續的發展或延伸研究上有兩個如前所述的建議。這個初步發展看起來是不錯的，我們論文的最終完整版本將結合其間一些學者所提供的建議，以便使其更為完整全面。我還計劃將最終版本提交到國際著名雜誌發表，相信這也是參加這個國際學術會議最顯著的收益。

在參加此次國際會議的討論中，我有以下的重要心得。實際現實生活中的雲端服務通常使用複雜的加密機制保護資料，攻擊者為了竊取企業的敏感資料，可能採取各種不同的攻擊模式侵入硬體。接著透過虛擬機（VM）越獄的方法，使其在虛擬機上執行某特定程式，允許在它運行的操作系統上，

從儲存媒介中恢復殘餘的資料。這些殘餘的資料可能會使得未經授權的用戶重建數據，並得以利用這個途徑獲得企業的敏感資料。防止 VM 越獄的方法已經被一些學者提出，它可以分析客戶 VM 是否被入侵或嵌入軟體。然而，資料殘留的問題還沒有很具體的機制來解決，如果用戶需要實際地消除在雲端磁碟中的文件的話，它是有必要有一個明確的資料處理機制。我們提出的公正第三者 (Trusted Third Party, TTP) 來監控資料處理整個生命週期的安全，就如同會計師提供審計過的財務資料一般，這個概念非常的棒，但更進一步考量的話則必須想辦法讓這樣的第三者報告有跟會計師簽證一樣的公信力，而這部份是一個很重要的延伸研究議題。我們拋出這個想法，希望也有學研界的先進們一起來思考這個問題。

在這次的報告中，我們提出了一個嶄新的基礎架構，它可以確保在雲端計算環境下，不使用的數據在客戶決定刪除他們時得以徹底清除。我們設計的主要優點是，客戶不需要改變他們原來使用網路的習慣。也就是說，這個安全操作的機制對最終用戶而言是透明的。新興的雲端計算技術需要保證各種安全要求否則大多數的客戶/組織將不敢採用。我們的研究提出了一個基礎架構來解決安全的問題，亦即數據的徹底清除。眾所周知，雲端計算的安全性符合要求後，才可以談管理和保障，而雲端計算服務的未來也方有前景可言。本研究嘗試為雲端計算的安全性投入心力，我們也希望這結果能夠引導未來在這一領域的研究。

## 附錄一



圖一 Keynote 1



圖二 Keynote 2



圖三 Presentation 1



圖四 Presentation 2



圖五 Presentation 3




圖六 與 Prof. Seweryn 合影

## 附錄二

# A Novel Infrastructure for Data Sanitization in Cloud Computing

**Dr. Cheng-Yuan Ku**  
Department of Information Management,  
National Chung Cheng University, Taiwan,  
R.O.C.

Date : May, 2013



# Outline

- I. Introduction
- 
- 
- 

# Background

- ◆ **Cloud computing service** ([Mell & Grance, 2011](#)):
  - IaaS , PaaS , SaaS
- ◆ **Cloud Security** ([Subashini & Kavitha, 2011](#)):
  - Data security
- ◆ **Personal Data Protection Act in Taiwan** ([Chang, 2012](#)):
  - Collecting, processing and using personal data
  - A party will be fined up to NT 200 million for violation.
  - Government agencies and non-governmental organizations must provide evidence for handling personal data with due care in the court. It is not the customer's responsibility.

# Motivations

- ◆ **Data Remanence :**
  - What is data remanence ?
    - Data sanitization ([Kissel et al., 2006](#))
    - One of the most important security issues for cloud computing
- ◆ **Comply with PDPA :**
  - Solutions for cloud computing
    - To provide evidence
    - To audit data security

# Outline

2. Related Technology and Works

# Cloud Computing Operating System

- Windows Azure  

- Google Apps  

- VMware vSphere  

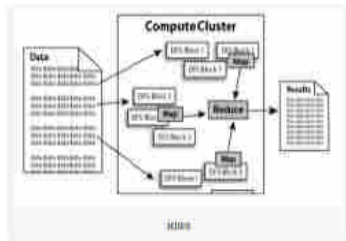
- Amazon WebService  


*VMware vSphere architecture*  
Source : Modified from the [VMware \(2011\)](#)



## Big Data Platform-Hadoop

- Hadoop Distributed File System (HDFS)
- MapReduce



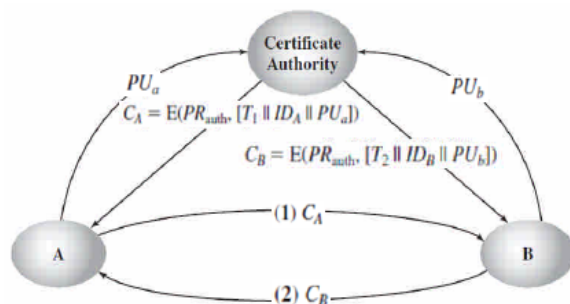
Hadoop cluster operating  
Source : [White \(2012\)](#)

## TTP in Cloud Computing

- ◆ Three major entities in trust model ([Zhu, Hu, Ahn, & Yau, 2011](#))

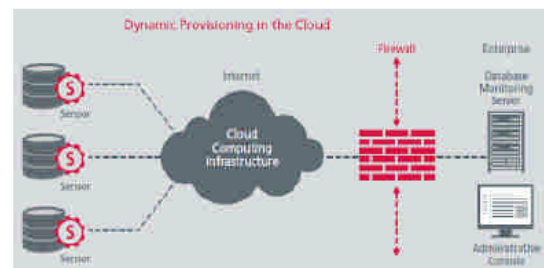
- Data Owner and Users
- Cloud Service Provider (CSP)
- Trusted Third Party (TTP)

## Public-Key Infrastructure



Public-key infrastructure model  
Source : [Stallings \(2012\)](#)

## Monitoring Approach for Cloud



McAfee database activity monitoring architecture  
Source : [McAfee \(2012\)](#)

## Data Sanitization (1/2)

- ◆ Definition ([Kissel, Scholl, Skolochenko, & Li, 2006](#)) :

- The data sanitization refers to removing remnant data from storage media.
- Type
  - Clearing : Overwriting
  - Purging : Degaussing
  - Destroying : Disintegration, incineration, pulverizing, shredding, and melting.

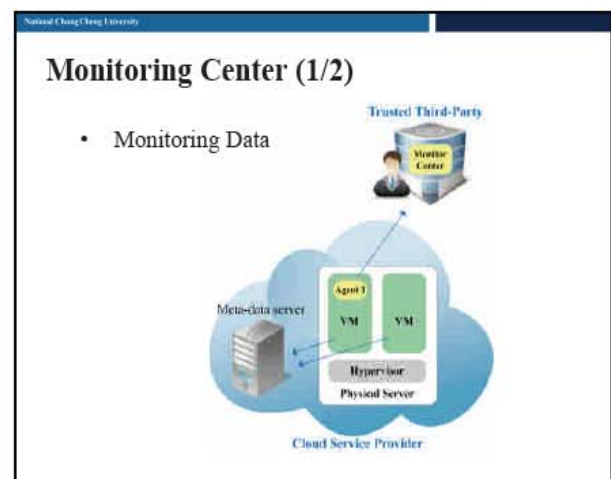
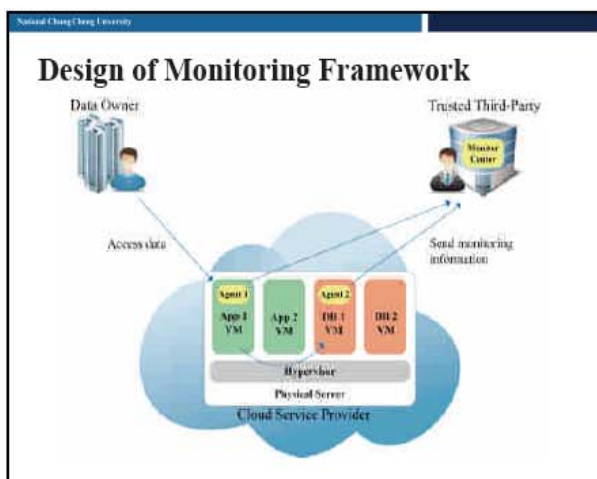
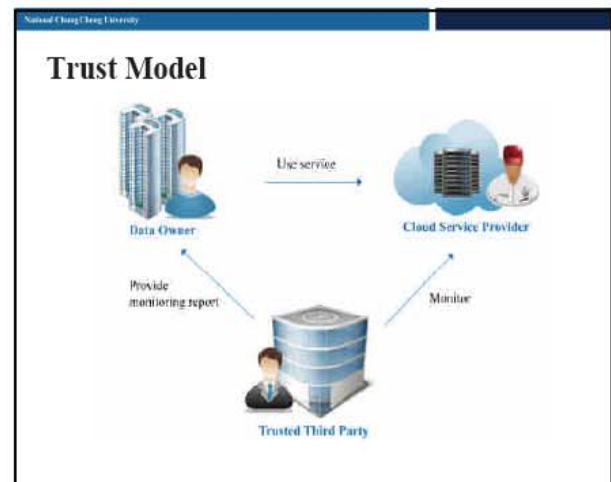
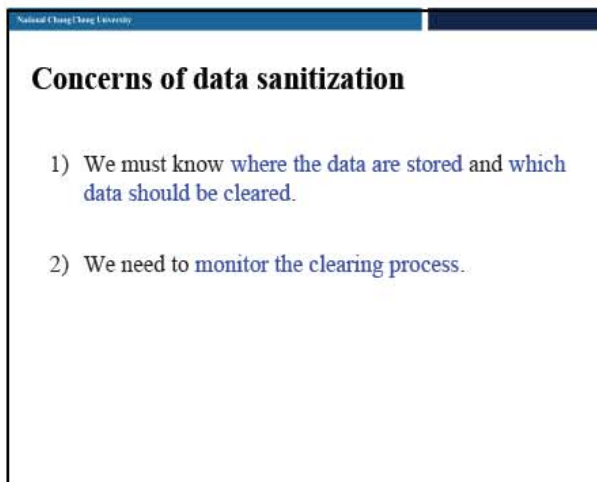
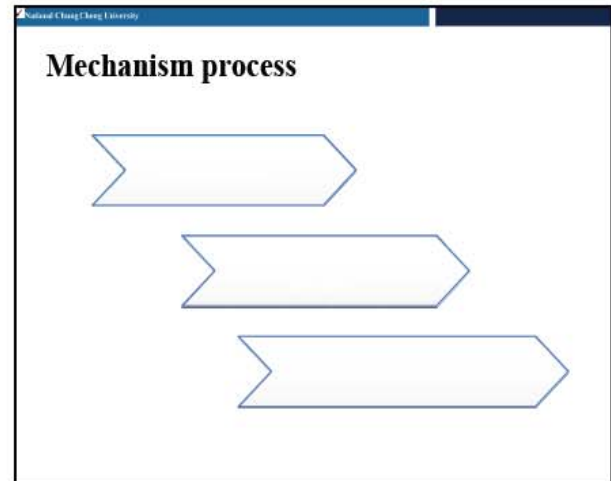
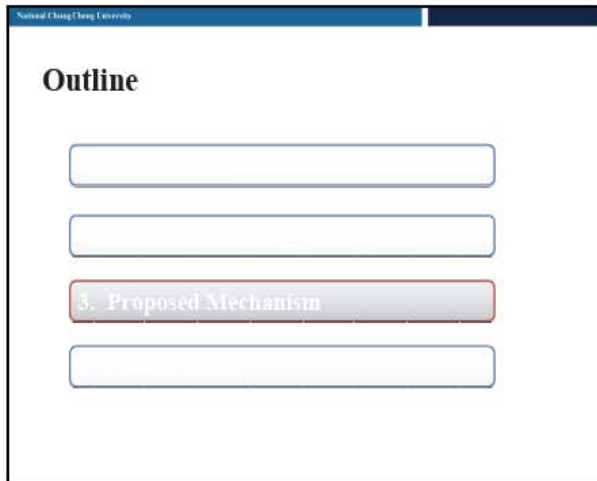
## Data Sanitization (2/2)

- ◆ Overwriting methods :

- Gutmann
- Schneier
- US DoD 5220-22-M
- VSITR

Overwrite Algorithm
<b>Pass 1:</b> Writes a zero and verifies <b>Pass 2:</b> Writes a one and verifies <b>Pass 3:</b> Writes a random character <b>Pass 4:</b> Writes a random character <b>Pass 5:</b> Writes a random character <b>Pass 6:</b> Writes a random character <b>Pass 7:</b> Writes a random character

Source : [US DoD 5220-22-M](#)



National Chung Cheng University

## Monitoring Center (2/2)

- Monitoring Data
  - Files content

File length <sup>(1)</sup>	Block size <sup>(2)</sup>	Replication <sup>(2)</sup>	Modification time <sup>(2)</sup>	Ownership <sup>(2)</sup>	Permission information <sup>(2)</sup>	File path <sup>(2)</sup>
<ul style="list-style-type: none"> <li>Monitoring Report               <ul style="list-style-type: none"> <li>Hadoop</li> </ul> </li> </ul>						

National Chung Cheng University

## Data Sanitization Scheme (1/2)

### ◆ Data Sanitization Process

```

graph TD
    DO[Data Owner] -- "1. Customer request for data sanitization" --> CSP[Cloud Service Provider]
    CSP -- "2. Overwriting the data and recovery test" --> DO
    CSP -- "3. The agents send monitoring records" --> TTP[Trusted Third-Party]
    TTP -- "4. Data sanitization monitoring report" --> DO
  
```

Package content :  $Cert_{TTP} \parallel Cert_{DO} \mid E(K_j, E(PR_{TTP}, [R_d \parallel T]))$

National Chung Cheng University

## Data Sanitization Scheme (2/2)

### ◆ Data Sanitization by Overwriting

- Customer interface and procedure
  - Interface provides customer two choices whether the data sanitization should be monitored or not.
  - Select the number of overwrites, and confirm the service.
  - Customers choose whether the recovery test report is necessary.

National Chung Cheng University

## Outline

4. Future Work

National Chung Cheng University

## Implementation and performance evaluation

- Monitoring agent
  - DAM (Database activity monitoring) captures the metadata packet
  - FAM (File activity monitoring) captures the log files
- Monitoring center
  - Provide  $\geq 64$  mega data or much larger to the monitoring center to test
- Overwriting program
  - To propose an efficient overwriting scheme in cloud

National Chung Cheng University

# Thank you for your attention

## 附錄三



Proceedings of 2013 International Conference on Technology Innovation and Industrial Management  
ISSN: 1906-7631

S2 - 142 <a href="#">[Full Text]</a>	Using sustainable competitive advantages to measure technological opportunities <i>Josu Takala, Matti Muhos, Sara Tilabi, Mehmet Serif TAS and Bingli Yan</i>
S2 - 164 <a href="#">[Full Text]</a>	The relationships among stocks, bonds and gold: safe haven, hedge or neither? <i>Shu-Mei Chiang, Chi-Tai Lin and Chien-Ming Huang</i>
S2 - 181 <a href="#">[Full Text]</a>	Warrant SEOs in an emerging market: evidence from Thailand <i>Pohwat Lerskullawat</i>
S2 - 197 <a href="#">[Full Text]</a>	Business justifications for rapid productisation in small- and medium -sized companies <i>Kai Hänninen, Matti Muhos and Harri Haapasalo</i>
S2 - 211 <a href="#">[Full Text]</a>	Institutional arrangement, technological innovation and application evolution: the rise of China's emerging computing infrastructure <i>Jiang Yu and Yue Zhang</i>
S2 - 239 <a href="#">[Full Text]</a>	Inter-organizational relationship and innovation performance in electronic supply chains <i>Jao-Hong Cheng, Chih-Ming Lee and Mu-Chung Chen</i>
S2 - 245 <a href="#">[Full Text]</a>	E-business analysis of real estate companies <i>Delvin Grant and Emna Cherif</i>
S2 - 257 <a href="#">[Full Text]</a>	Exploring the dynamic interdependence in the east Asian stock markets <i>Suthawan Prukumpai and Yuthana Sethapramote</i>
S2 - 279 <a href="#">[Full Text]</a>	Organizational learning: a mediating factor between technological innovation and TQM <i>Voon-Hsien Lee, Keng-Boon Ooi, Chee-Keong Choong and Kee-Luen Wong</i>
S2 - 282 <a href="#">[Full Text]</a>	Determinants electricity demand in industry and households <i>Štefan Bojnec and Drago Papler</i>
S2 - 283 <a href="#">[Full Text]</a>	Developing credit rating indicators of customers for electronic companies <i>Hsiao-Chen Chang, Kuang-Hsun Shih, Ming-Fang Lee and Yi-Hsuan Chou</i>

### Session 3: Management of technology and innovation- applications, cases, and new product/ service development

S3 - 1 <a href="#">[Full Text]</a>	Supervision and protection of e-data in sensitive information systems <i>Vladimir Šimović, Matija Varga and Marin Milković</i>
S3 - 25 <a href="#">[Full Text]</a>	A novel infrastructure for data sanitization in cloud computing <i>Cheng-Yuan Ku and Yu-Siang Chiu</i>





Proceedings of 2013 International Conference on  
Technology Innovation and Industrial Management  
29-31 May 2013, Phuket, Thailand

### A NOVEL INFRASTRUCTURE FOR DATA SANITIZATION IN CLOUD COMPUTING (RESEARCH PAPER)

Cheng-Yuan Ku, National Chung Cheng University, Taiwan, ROC  
E-mail: cooper.c.y.ku@gmail.com

Yu-Siang Chiu, National Chung Cheng University, Taiwan, ROC  
E-mail: fishfly1115@gmail.com

#### ABSTRACT

**Purpose-** In this extended abstract, we propose a novel infrastructure in cloud computing environment which assures the data sanitization after the customers decide to delete them.

**Design-** A mechanism with monitoring agents is suggested to watch the data usage over entire life cycle and assure the data sanitization in the end.

**Findings-** Security analysis and performance analysis will be done after the complete infrastructure is decided. We expect this mechanism should fulfill the security and performance requirements for cloud computing users.

**Originality/Value-** The emerging cloud computing technology needs the assurance of various security requirements, otherwise most of customers/organizations do not dare to adopt it. Our research proposes an infrastructure to solve one of the security problems, i.e. data sanitization. As well known, only after the security requirements of cloud computing could be managed and guaranteed, the prospects of the cloud services are brightening.

**Keywords:** cloud computing, cloud services, information security, data sanitization, trusted third party (TTP), agent

#### INTRODUCTION

In recent years, as cloud computing becomes more and more popular, it has gradually drawn many enterprises' attention. Ironically, one of the major factors which lead the development of cloud computing is the previous economic recession. Due to the keen business competition and tight budget, enterprises need to find any possible ways to reduce cost. According to the National Institute of Standards and Technology (NIST), cloud computing providers offer services with three fundamental models (Mell and Grance, 2011):

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Based on the individual need, enterprises can choose anyone, both or all of the above-mentioned methods to construct computing services for stakeholder. From the perspective of technology, cloud computing seems to be able to give a chance to divest infrastructure management of information systems and to enhance core competencies. However the potential security issues may hinder the cloud services from fast developing.

Even with the protecting mechanism in cloud, the attacker still can take various attack models to invade. Cloudburst virtual machine (VM) escape is an exploit method that enables



a guest-level virtual machine to attack its host (Kortchinsky, 2009). A method that prevents the VM escape has been proposed by security researchers (Ristenpart et al., 2009). In addition to the above-mentioned attack, one of the other major security considerations is data sanitization. Actually a deleted file only means the erased directory, not the file itself. This issue becomes even more complicate in cloud environment and still has no concrete solutions until now.

The trusted third party (TTP) and agent are two of the popular methods to solve many security issues. The TTP can act as a monitor and audit the performance of service providers for customers. An agent is generally developed to monitor network activity, collect information, act for a user or other program ... and so on. For example, it can identify malicious network behavior that does not comply with the policy and send the alert to the managing center (Manzoor and Nefti, 2009). According to the published security guidance in cloud computing by Cloud Security Alliance (CSA) (CSA, 2011), there are two types of monitoring mode:

- Database Activity Monitoring (DAM) : Database Activity Monitor captures and records all Structured Query Language (SQL) activity in database in real time or near real time. The database monitoring server will generate alerts on policy violations.
- File Activity Monitoring (FAM) : FAM records how the customers access file and generate alerts on policy violations.

Until now, there are some solutions of new generation DAM which are based on kernel-level implementations and other intrusive approaches (Lombardi and Di Pietro, 2011; Shao et al., 2010). This means that adding a layer of security requires changes in architecture and relies on the virtualization technology. McAfee, the world's largest dedicated security technology company, has made an effective solution which can be easily embedded into the guest VM. This is the so-called McAfee Database Activity Monitoring (McAfee, 2012). In short, within the proposed infrastructure, the TTP, agent modules and improved sanitization procedure are adopted to assure the security of sensitive data.

### **PROPOSED MECHANISM**

In order to achieve the data sanitization, the entire data life cycle must be monitored. In this way, the manager can record and control the detailed process of data usage and storage. Based on the above-mentioned McAfee Database Activity Monitoring, we further design a monitoring mechanism to handle the data sanitization problem as shown in Figure 1. In cloud environments, the customers, in general, deploy the needed applications, platforms or infrastructures on VMs. Therefore, we suggest that a monitoring agent should be embedded into every VM which hosts the application or database.

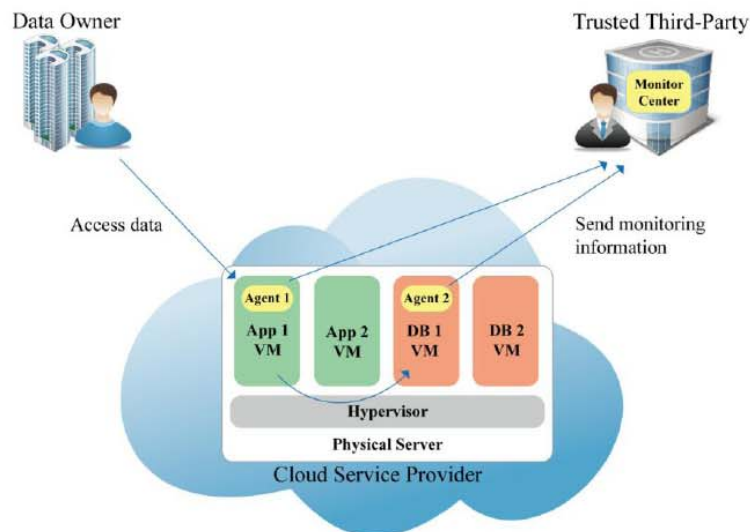


Fig. 1 Monitoring architecture

- Access function : while the data owner accesses data via applications on VM, agent 1 shall collect the log information and sent to the TTP.
- Process function : agent 1 shall also monitor communication between the applications and database.
- Store function : agent 2 shall monitor the database and have all activity reports sent to TTP.

## FUTURE WORKS

Currently the design of monitoring mechanism in cloud environment is already finished but the detailed data sanitization procedure is still under construction. Furthermore, the security analysis and performance analysis should be conducted thereafter. The security analysis is going to include the man-in-the-middle attack, verifiability, brute-force attack, and spoofing and so on. We plan to implement the prototype of proposed mechanism by using Hadoop platform. As for the performance analysis, the speed of overwriting and the efficiency of monitoring center will be assessed. Finally, we will compare with McAfee Database Activity Monitoring about performance.

## REFERENCES

1. CSA (2011), "Security guidance for critical areas of focus in cloud computing v3.0", Cloud Security Alliance.
2. Kortchinsky, K. (2009), "CLOUDBURST: A VMware guest to host escape story", Black Hat USA, Las. Vegas, USA, June 2009.
3. Lombardi, F., and Di Pietro, R. (2011), "Secure virtualization for cloud computing", Journal of Network and Computer Applications, Vol. 34 No. 4, pp. 1113-1122.
4. Manzoor, U., and Nefti, S. (2009), "An agent based system for activity monitoring on network-ABSAMN", Expert Systems with Applications, Vol. 36 No. 8, pp. 10987-10994.





**Proceedings of 2013 International Conference on  
Technology Innovation and Industrial Management  
29-31 May 2013, Phuket, Thailand**

5. McAfee (2012), "Database security in virtualization and cloud computing environments", McAfee.
6. Mell, P., and Grance, T. (2011), "The NIST definition of cloud computing", NIST Special Publication 800-145.
7. Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. (2009), "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds", in the 16th ACM Conference on Computer and Communications Security Proceeding of the International Conference in Chicago, IL, USA.
8. Shao, J., Wei, H., Wang, Q., and Mei, H. (2010), "A runtime model based monitoring approach for cloud", presented at the 2010 IEEE 3rd International Conference on Cloud Computing.