雲端安全儲存系統

林華鵬　周國森　郭志勇　單張麟　陳彥仲　林宗毅
中華電信研究院　資通安全研究所　雲端運算研究所
walterlin@cht.com.tw、cksp@cht.com.tw、jason_kuo@cht.com.tw、zlshan@cht.com.tw、yzchen@cht.com.tw、ianlin@cht.com.tw

摘要

近年來雲端運算技術在資訊科技產業上已成為眾所皆知的技術，雲端技術服務提供了有效率及有彈性的資源分配，使用者可以依據自己的資源需求，動態的取得資源，如此使用者僅需依實際上使用資源量的多寡來支付費用。另一方面，許多企業因擁有大量的數位資料，原本可能需要花費龐大的成本來購買硬體儲存設備，然而因為雲端技術服務用多少付多少的特性，可有效的減少企業購買硬體儲存設備的成本。

雖然企業使用雲端儲存服務可有效降低成本，但將可能會有企業敏感性資料散佈在世界各地儲存設備上之安全性疑慮。

資料安全是企業及個人都相當重視的重要議題，且雲端資訊安全和實體資訊安全擁有不同的特質與需求，本文將提出一個雲端安全儲存系統，能夠有效解決雲端儲存服務所面臨的資訊安全議題，確保雲端儲存服務使用者的資料安全。

關鍵詞：雲端運算、雲端儲存服務、雲端儲存安全、資料安全、加密與解密

Abstract

In recent years, cloud computing has become the well-known technology in the information technology industry. The cloud-based services always supply great service performance and flexible resource allocation to the cloud users. Therefore, users can dynamically allocate the storage resources and computing according to the demands. It saves huge hardware costs and users only need to pay for what they really used. On the other hand, a number of companies plan to paper information data into digital data, so the data storage and backup requirements are highly valued. It would take considerable cost if the companies build their own storage. Although cloud storage services could effectively reduce the costs, users are afraid of the data to be stolen through the accessible Internet, especially for the sensitive data.

Data security in the cloud is an important issue for companies and personal users. In this paper, we will propose a cloud security storage system to solve those security issues to ensure that the user's data security.

Keywords: Cloud Computing、Cloud Storage、Security of Cloud Storage Services、Data Security、Encrypt and Decrypt

1. 前言

「雲端技術」已成為近年來最熱門的名詞，政府也投入龐大的經費，投入雲端運算的領域，當然中華電信也不缺席，在 2013 年 6 月耗資 130 億元打造的中華電信 IDC 雲端資料中心，預定 2015 年正式營運並提供服務，預估在四年之內就有上千億元的雲端建設投資將陸續進駐。

另一方面，由台灣雲端運算產業協會規劃建置的「台灣雲谷」已經在 2012 年 3 月 14 日正式啟用，未來能夠整合雲端產業資源並提供企業完整的雲端服務解決方案。

雲端儲存屬於雲端運算大架構中的一環，所謂雲端運算就是將具備擴充性及彈性化的 IT 資源，透過網路並以服務的型態分派給用戶的一種運算服務型態。相同的，所謂雲端儲存，也就是將具備高擴充性與高彈性化的儲存資源存放到網際網路上供用戶存取的一種服務型態。進一步而言，雲端儲存由儲存服務提供商(SSP；Storage Service Provider)所提供，雲端儲存擁有彈性的儲存空間池(Storage Pool)管理架構，比起傳統儲存架構或裝置，雲端儲存將會更加便宜。

為因應企業龐大的數位資訊，雲端儲存服務帶給企業更有彈性及更節省成本的解決方法，但相較於傳統儲存設備，原本企業擁有的個資或機敏資料是儲存於企業內部儲存設備，若遺失或遭竊都是企業本身的責任，但若企業將機敏資料或個資存放於雲端儲存服務提供商之儲存空間，企業便無法保證資料安全性問題，當資料毀損或遺失，又或是敏感性資料遭到公開散佈，將會面臨到各種的資訊安全性議題，導致企業及個人使用者對雲端儲存望而卻步。

企業將資料儲存於第三方雲端儲存服務提供商，將面臨到「資料是否會遺失」、「資料是否會遭駭客入侵竊取」、「資料是否會被第三方讀取甚至公開」、「資料是否會被複製或備份到其它未知的伺服器」、「若退租第三方是否會將資料確實移除」、「由檔案名稱判斷可能為敏感性資料」等等的安全議題，為了使雲端儲存能為企業所接受，使得企業願

意將敏感性資料存放在雲端儲存服務提供商儲存空間，必須解決前述的雲端儲存資訊安全之議題。

本研究將提出一個雲端安全儲存系統，可有效的解決上述提到之安全議題，使得雲端儲存達到資料機密性、資料完整性等安全優勢，進而增強使用者對雲端儲存之信賴度。

2. 相關研究

2.1 雲端儲存簡介

雲端運算基本上是使用網際網路的方式調配資源，使用者不需要知道雲端中底層基礎設施的詳細資訊，也不需要具備相關專業知識，即可透過網際網路動態的取得所需要的資源。

雲端儲存基於雲端運算的概念，由第三方雲端儲存服務提供商，提供雲端儲存空間，所有伺服器及儲存資源都由第三方代管，第三方提供像是儲存資源池的概念，使用者可依需求購買或租賃儲存空間，即可動態的取得所需的儲存資源，並將檔案資料存放到儲存空間中，而檔案資料可能被第三方利用分散式儲存的方式，分散儲存在多部的伺服器主機上。

一般使用者可以透過第三方雲端儲存服務提供商所提供的瀏覽器 Web 化介面，或是使用第三方所提供的服務應用程式介面(API)的方式，對後端雲端儲存空間進行存取，企業只需要依實際使用的空間量來支付相關費用，如此企業不需要負擔儲存設備的購買及管理成本，可有效減少企業數位資料的儲存成本。

2.2 雲端運算類型

根據雲端資訊安全聯盟(CSA: Cloud Security Alliance)[1]於雲端安全重點領域指引文件中的定義，雲端運算分為三種產業類型模式：

●基礎架構即服務(IaaS: Infrastructure as a Service)：使用者不需自行購買硬體建置基礎設施，即可透過租用的方式，使用虛擬化處理器、儲存容量、網路等基礎之運算資源。

●平台即服務 (PaaS: Platform as a Service)：可提供雲端軟體平台開發人員所需的程式語言工具或其它相關工具，使其能在基礎架構上部署及開發應用程式，建立自己的功能平台(如規畫設計、開發、測試、部署等)，使用者僅需要控制部署環境設定組態，不需要知道較底層的網路、處理器等基礎架構。

●軟體即服務(SaaS: Software as a Service)：使用者可以透過任何具有瀏覽器的設備，設備本身不需要強力的硬體效能，不需要下載或安裝額外的程式，亦不需瞭解或管理底層的雲端基礎架構，即可直接存取該應用軟體程式。

2.3 雲端儲存安全議題

2.3.1 雲端儲存安全調查報告

IT 研究與分析網站 InformationWeek Analytics[2]於 2011 年 6 月的一份調查報告指出，企業害怕使用公用雲端儲存最大的原因在於「雲端儲存安全性的顧慮」(73%)，企業內部可能擁有機敏性資料，或是個資相關資料，即使雲端儲存方案可以有效的降低企業購買及管理儲存設備的成本，但可能因擔心敏感性資料遭第三方使用或公開散佈，或儲存空間遭到駭客入侵等安全性議題，導致企業對雲端儲存服務的使用上仍有疑慮。

2.3.2 傳統儲存架構與雲端儲存架構

圖 1 為傳統儲存架構與使用雲端儲存架構之示意圖，說明如下：

●傳統儲存架構：傳統的儲存架構模式，是透過遠端磁碟或 FTP 的方式，對企業內部的儲存設備進行存取，缺點在於使用者必須安裝特殊協定的客戶端軟體工具，且企業必須自行負擔購買儲存設備成本，以及管理設備的成本。

●雲端架構-使用瀏覽器：用戶利用瀏覽器(如 Firefox、Internet Explorer、Chrome、Safari 等)對雲端儲存空間直接進行存取，但企業將內部機敏性資料存放於雲端儲存空間，將會有資料外洩的疑慮，一方面擔心是否會被雲端儲存服務提供商公開或使用，另一方面擔心是否會遭到駭客入侵而遺失資料。

●雲端架構-使用 Client 應用程式：用戶使用 Client 應用程式(如 CrossFTP、Dragon Disk、JetS3t 等)對檔案進行上傳的動作，雖然有部份 Client 應用程式有實作資料加密的功能，但因用戶必須依應用程式的類型安裝相對應的程式語言編譯器才可使用應用程式工具，相較起來其方便性較沒那麼友善。

●雲端架構-使用雲端安全儲存系統：用戶透過本研究所提供的雲端安全儲存系統進行檔案上下載，用戶可透過雲端安全儲存系統所提供的瀏覽器

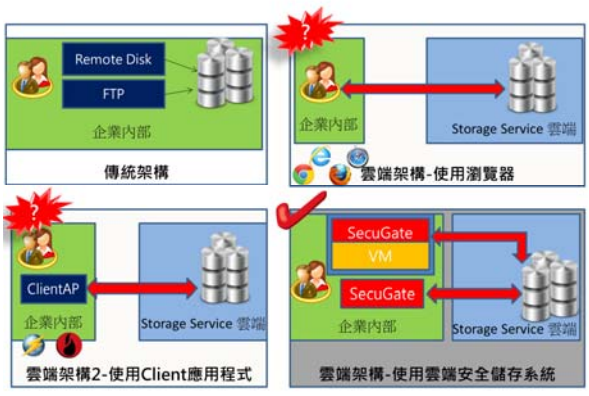

圖 1 傳統儲存架構與雲端儲存架構圖

介面或 WebDAV(VDisk/NFS)的介面進行檔案上下載的動作，當檔案經過雲端安全儲存系統時，將自動化實施資訊安全強化機制處理後，才可儲存到後端雲端儲存服務提供商儲存空間，因經過資安強化處理，所以雲端儲存服務提供商無法得知檔案正確內容，即使雲端儲存空間遭駭客入侵，同樣無法得到資料的正確內容。

2.3.3 雲端儲存安全問題

本研究經過資料蒐集匯整後，整理出企業使用雲端儲存服務可能會遭遇到的安全問題所列如下：

●雲端儲存服務身份認證安全性問題：若使用雲端儲存服務，一般雲端儲存服務提供商將會提供一組帳號密碼的金鑰給使用者，使用者則可以透過這組帳號密碼對雲端儲存空間進行存取，但一旦這組金鑰遭到有心人士竊取，則儲存空間上之敏感性資料也可能遭到取得。

●用戶所能掌控之安全範圍邊界問題：傳統上企業將機敏性資料存放在企業內部的儲存設備上，因此企業可以自行完全掌控其資料的安全範圍，但若使用雲端儲存服務，則企業必須信任第三方雲端儲存服務提供商不會使用或散佈企業內部的機敏性資料。

●檔案資料最終存放位置的疑慮：傳統上企業將機敏性資料存放在企業內部的儲存設備，企業可明確的知道檔案所在的位置，但若使用雲端儲存服務，檔案資料可能因為分散式檔案系統的特性，資料被複製或備份到未知的伺服器上，一旦用戶退租雲端儲存服務，也無法確定機敏性檔案資料是否已確實完全的被刪除。

●檔案資料完整性的疑慮：傳統上企業直接將資料存放在企業內部的硬體儲存設備上，不需要透過網際網路即可直接在企戶內部儲存設備上確認檔案的完整性，但若使用雲端儲存服務，必須透過網際網路將檔案資料上傳至雲端儲存空間，則可能會因網路穩定性或網路品質問題，造成封包資料的遺失，而檔案完整性出現問題。

●雲端儲存空間資料被駭客竊取並散佈：傳統上企業可使用安全設備，加強存放機敏性資料的儲存設備，若使用雲端儲存服務，則企業用戶必須全盤信任第三方雲端儲存服務提供商的安全性防護機制，可以有效防護駭客的入侵。

3. 雲端安全儲存系統架構

3.1 雲端安全儲存系統使用情境

圖 2 為雲端安全儲存系統使用情境示意圖，雲端安全儲存系統提供了瀏覽器介面(支援 HTTP/HTTPS 協定)，讓所有擁有瀏覽器的設備皆可以透過此介面，將檔案資料透過瀏覽器上傳至後端雲端儲存空間，另外使用者也可以透過 WebDAV(VDisk/NFS)的介面，使用類似網路芳鄰的方式，將檔案資料上傳至後端雲端儲存空間。

當檔案經由雲端安全儲存系統時，會將檔案資料進行資訊安全強化的特殊處理，處理完成後，才會將檔案資料送至第三方雲端儲存服務提供商，第三方雲端儲存服務提供商看到的只是沒有任何意義的資料片段，無法得知檔案實際的內容，因此雲端儲存服務提供商並無法得知檔案真正內容。

同樣的，使用者或企業可透過瀏覽器或 WebDAV(VDisk/NFS)的介面，來對檔案進行下載的動作，檔案經過雲端安全儲存系統後，將對原本沒有意義的資料片段實施還原的動作，使用者即可獲得原始的檔案資料內容。

3.2 雲端安全儲存系統架構

圖 3 為雲端安全儲存系統架構圖，使用者透過前端使用者介面，進行檔案的上傳及下載，雲端安全儲存系統中的資訊安全強化模組則負責接收前端使用者介面所傳送過來的資訊，並且對使用者準備傳送或接收的檔案進行資訊安全的強化，不論上傳或下載，資訊安全強化模組皆會與雲端儲存服務提供商進行溝通，並傳輸或取得檔案，而後端雲端儲存服務提供商可以是各種不同的 S3 Compatible 之服務提供商。

圖 2 雲端安全儲存系統使用情境示意圖

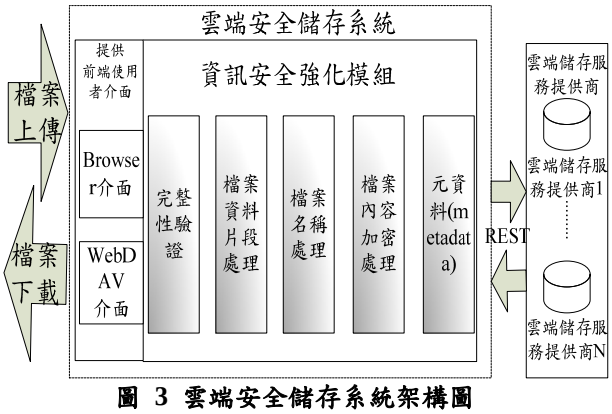

圖 3 雲端安全儲存系統架構圖

使用者可透過前端使用者瀏覽器介面或WebDAV 協定(VDisk/NFS)介面，選擇想要上傳至雲端儲存空間的檔案，檔案將透過介面被傳送到資訊安全強化模組，資訊安全強化模組將對檔案實施資安強化處理。

檔案資料於資訊安全強化模組中將實施完整性驗證、檔案資料片段處理、檔案名稱處理、檔案內容加密處理，最後將各個片段檔案名稱與原始檔案名稱實施對應，儲存在使用者可自行控管的元資料(MetatData)檔案中，如此即完成資訊安全強化模組對檔案實施強化的步驟。

資訊安全強化模組會再將資安強化後的檔案片段，利用多工的方式，將各個檔案片段使用 REST 協定傳送至後端各種支援 S3 Compatible 的雲端儲存服務提供商，也因各個上傳完成的檔案片段皆經過資訊安全強化模組的安全強化處理，所以後端的雲端儲存服務提供商無法得知實際檔案資料的內容。

同樣使用者也可透過前端瀏覽器或WebDAV(VDisk/NFS)介面，下載並取得原始檔案內容，存放於雲端儲存服務提供商的檔案片段，將被傳送至雲端安全儲存系統的資訊安全強化模組實施反向的處理，檔案將會被還原成原始內容，呈現在前端使用者介面上。

4. 雲端安全儲存系統功能

4.1 雲端安全儲存系統瀏覽器介面實作

圖 4 為雲端安全儲存系統瀏覽器介面功能圖，透過雲端安全儲存系統所提供的瀏覽器介面存取後端雲端儲存空間，其介面上所提到的功能，於表 1 雲端安全儲存系統瀏覽器介面功能介紹表上進行詳細說明：

表 1 雲端安全儲存系統瀏覽器介面功能介紹表

功能名稱	功能詳細說明
分享密庫	分享自己的密庫給其他雲端安全儲存系統的使用者
開啟或關閉密庫	開啟或關閉屬於自己的密庫
刪除密庫	將未使用的密庫刪除
進入密庫	顯示所有存在於該密庫中之檔案列表，並進一步對檔案進行操作。
編輯密庫說明	對該密庫的用途作描述
上傳檔案	在本機端，選擇想要上傳至雲端儲存空間之檔案，檔案傳送過程中，會經由雲端安全儲存系統之安全強化處理，所以成功傳送至雲端儲存空間之檔案是具備資料安全性的
刪除檔案	於檔案列表中刪除所選擇的檔案，檔案也隨之在後端儲存空間被刪除
重新命名檔案	檔案名稱將被重新命名
下載檔案	從雲端儲存空間中，取得原始檔案內容
分享檔案	分享自己的檔案給其他雲端安全儲存系統的使用者

4.2 雲端安全儲存系統 WebDAV 介面實作

雲端安全儲存系統除了實作瀏覽器介面外，也有另外實作 WebDAV 的介面，圖 5 為雲端安全儲存系統 WebDAV 介面圖，於表 2 雲端安全儲存系統 WebDAV 介面介紹表上進行詳細說明：

圖 4 雲端安全儲存系統瀏覽器介面功能圖

圖 5 雲端安全儲存系統 WebDAV 介面圖

表 2 雲端安全儲存系統 WebDAV 介面介紹表

Windows WebDAV	Mobile Device WebDAV
圖 5 左側為使用 Windows 內建的 WebDAV 協定，連接到雲端安全儲存系統提供之 WebDAV 介面，可以透過拖曳資料夾或拖曳檔案的方式，將檔案上傳至後端雲端儲存空間，上傳途中同樣的檔案會經過資訊安全強化模組的安全強化	同樣的可以在支援 WebDAV 的行動裝置上，使用 WebDAV 協定連接到雲端安全儲存系統的介面上，使用者可在行動裝置上，安裝 WebDAV 協定之 APP，圖 5 右側為使用 iPhone 行動裝置配合 WebDAV APP，對雲端安全儲存系統實施操作的展示

4.3 雲端安全儲存系統資訊安全強化結果

圖 6 為雲端安全儲存系統資安強化結果確認圖，使用者透過雲端安全儲存系統，上傳多個文字檔案，檔案經過資訊安全強化模組對檔案資料實施安全性強化後，才上傳至後端雲端儲存空間。我們利用開放原始碼的 S3 客戶端工具 JetS3t ，直接連接到後端雲端儲存服務提供商，實際檢視上傳後的檔案內容，可發現檔案內容已實施資安強化處理。

在經過雲端安全儲存系統資安強化處理後的檔案，不僅檔案名稱被置換成無意義的檔名，並且檔案也成為許多無意義的檔案片段。為了進行確認，將檔案片段下載後，直接開啟檔案片段內容，可以發現資料內容是呈現密文的情況，因此即使檔案是儲存於不信任的第三方雲端儲存服務提供商，或是後端儲存空間若不幸遭到駭客入侵，也無法還原其原始檔案的真正內容，因此可以確保在後端雲端儲存空間檔案的安全性。

同樣地，當使用者進行儲存空間退租時，因後端是經由資訊安全強化模組處理後的資料，所以即使實際上資料片段沒有被第三方雲端儲存提供商真正刪除，或是檔案被複製或備份至其它伺服器時，同樣不需要擔心機敏性資料外洩的問題。

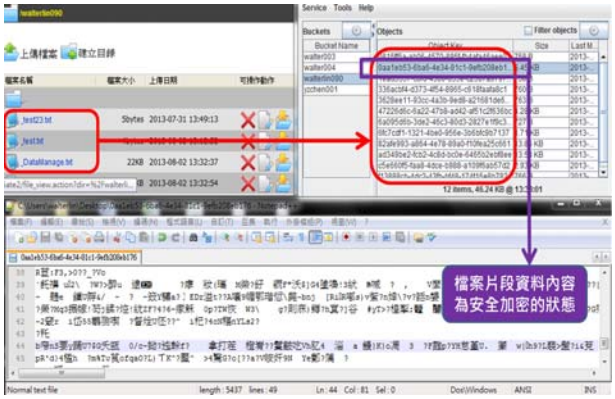

圖 6 雲端安全儲存系統資安強化結果確認圖

4.4 雲端安全儲存系統優勢

雲端安全儲存系統可確保檔案資料於雲端儲存空間之機密性、完整性、刪除確定性。綜合來說，雲端安全儲存系統具備的優勢於表 3 雲端安全儲存系統優勢列表進行說明：

表 3 雲端安全儲存系統優勢列表

優勢項目	功能詳細說明
雲端平台具高度獨立性	雲端安全儲存系統可運行於 XEN、VMWare、KVM…等平台之虛擬機器上
與作業系統之相容性	雲端安全儲存系統建置於 Tomcat Web 伺服器上，並使用 Java 程式語言所開發，可運行於 Linux、Windows…等作業系統上
使用者自行控管金鑰及安全性範圍	使用者可以自行保管加解密之金鑰，所有加解密過程在用戶端進行，可確保檔案資料之機密性
加密等級高	使用高強度之 AES-256 對稱式加密演算法並配合非對稱式加密演算法
通道安全	所有檔案傳輸過程，皆運行於 SSL 安全通道上
使用 Smart Card 認證	企業可選用 Smart Card 認證機制，透過 Smart Card 安全認證後才可使用雲端安全儲存系統
檔案操作權限控管	可限制雲端安全儲存系統使用者檔案操作權限，如可讀/寫、可瀏覽之副檔名
操作紀錄查詢	提供雲端安全儲存系統之操作紀錄查詢功能
標準化之存取介面	提供 HTTP/HTTPS 及 WebDAV 之存取介面，使得具備瀏覽器及支援 WebDAV 協定之機器及行動裝置設備，可透過此兩種存取介面進行檔案上下載之操作
分享機制	提供檔案目錄分享機制，以及限制下載次數之單一 URL 分享機制
片段分散儲存機制	具備將單一檔案進行若干片段處理並傳送至不同雲端儲存服務提供商儲存空間之機制

5. 結語

資訊科技與網路技術不斷的提升，促成了雲端服務時代的來臨，使得雲端服務成為近來最熱門的話題，隨著企業實體資料轉換為數位化資料的趨勢，企業必須購買更多的儲存設備來儲存龐大的數位資料，可能增加了企業購買儲存設備及維運的成本。

企業若使用雲端儲存服務，可視實際需求調整儲存空間的租用量，並依據租用量來計費，如此可有效降低購買實體儲存設備的資本支出及維運設備的人事成本，但雲端儲存是否會被企業所接受，企業主要考量仍在於能否解決雲端儲存資訊安全方面的議題。

雲端儲存服務所衍生的資訊安全問題與以往傳統資訊安全領域不盡相同，例如檔案資料最終存放位置的疑慮、檔案資料完整性的疑慮、檔案資料被駭客竊取並散佈的疑慮、若退租是否真的將檔案資料刪除的疑慮。若企業的機敏性檔案資料未實施安全強化處理，直接將檔案資料儲存於雲端儲存空間，若不幸重要資料被公開或外洩，將造成企業嚴重的損失。

本研究提出雲端安全儲存系統，使用者可直接使用任何具有瀏覽器之設備，或支援 WebDAV 協定之設備，對後端儲存空間進行存取，所有透過雲端安全儲存系統上載至雲端儲存空間之檔案資料內容，均經過資訊安全強化模組的處理，可確保後端雲端儲存空間資料的安全性，達到資料機密性、資料完整性、資料刪除確定性等安全儲存的目的。

雲端儲存服務帶給使用者及企業更大的便利，使用雲端安全儲存系統能夠解決使用者及企業所擔心的雲端儲存安全議題，並爲雲端儲存使用者提供更完整的安全保障，增強使用者對雲端儲存之信賴度，助益雲端儲存技術之推廣。

參考文獻

[1] Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing V3.0”, 2011.

[2] Michael Biddick, “Cloud Storage: Changing Dynamics Beyond Services”, 2011.

[3] Grant Bugher, “Secure Use of Cloud Storage”, USA: Blackhat Briefings 2010.

[4] Rampal Singh, Sawan Kumar, Shani Kumar Agraharii, “Ensuring data storage security in Cloud Computing”, International Journal Of Engineering And Computer Science, 2013, pp. 825-830.

[5] Amazon, “Amazon Web Services: Overview of Security Processes”, AWS Security Whitepaper, 2011.

[6] Google Developers, “Google Cloud Storage, https://developers.google.com/storage/”, 2013.

[7] Cloud Security Alliance, “Top Threats to Cloud Computing V1.0”, 2010.

[8] Ceph, “Ceph Storage File System, http://ceph.com/ceph-storage/file-system/”, 2013.

[9] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing”, CA: INFOCOM, 2010, pp. 1-9.

[10] S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing”, Journal of Network and Computer Applications, 2011, pp. 1-11.

[11] L.M. Kaufman, ”Data Security in the World of Cloud Computing”, Security & Privacy, IEEE, 2009, pp. 61-64.

[12] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou, “Security and Privacy in Cloud Computing: A Survey”, Beijing: Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on, 2010, pp. 105-112.