一個 Push 模式的網路資料安全查詢與傳輸平台

周忠信、郭士彰、范明翔

東海大學資訊科學系

TEL:(04)3590121 EXT. 3296

EMAIL: jwo@s867.thu.edu.tw

簡仲璟

台灣省交通處港灣技術研究所

TEL:(04)6564216 EXT. 411

EMAIL: java97@cis.thu.edu.tw

摘要

隨著網際網路技術的快速發展，透過全球資訊網來查詢或擷取資料，已逐漸 成爲一種相當受歡迎且方便的方式。然而在網路上的資料，有些是有價值或必須 受到主管機關審核通過後才可下載取得。未經許可的資料部分，使用者不得任意 獲得。另外由於網際網路本身是一個公用的開放網路架構，被同意下載的資料必 須能夠保證不被其他未授權使用者於網路傳輸時擷取。因此本研究之主要目的即 在利用全球資訊網之 Push 模式並透過 Java 語言，實際發展出一套既能夠保護 網站本身安全，且能保障資料不被未經授權人士從網站或於網路傳輸時所擷取的 網路資料傳輸平台。本研究之結果，目前已實際應用於台灣省交通處港灣技術研 究所的海氣象資料庫查詢系統上。同時它也可以輕易地被應用在目前廣爲使用的 線上軟體買賣上。

1. 背景簡介

自從 1989 年 Tim Berners-Lee 將全球資訊網 (World Wide Web ， WWW) 帶 入網際網路 (Internet) 後，全球資訊網在各種領域上的發展，即如雨後春筍般地 出現。其中透過網路獲得資料或進行資料查詢，更是全球資訊網上的主要應用之一。 這些資料的種類包羅萬象，例如像股市資料或政府法令規章等，對網路上的使用者 而言是一種重要的資訊服務。然而隨著網際網路的實際應用越來越爲成熟後，透過 企業內網路 (intranet) 或所謂的企業外網路 (extranet) 傳輸機密或是有價資料 的情形將逐漸普及。舉例來說，國稅局有關全國納稅人之納稅資料可以直接放在其 企業內網路上，供檢調人員能隨時透過網際網路快速查詢或使用以協助犯罪之調查。 然而檢調人員並非所有資料皆可獲得，他們必須在申請後只能查詢獲授權部分之資 料。同時由於網際網路本身是一個公用的開放網路架構，被同意下載的資料必須能夠保證不被其他未授權使用者於網路傳輸時擷取。而這樣的網路資料傳輸環境，才 能保障全體納稅義務人的隱私權，但同時又能提供及時的資訊服務以協助打擊犯罪。 在企業內網路或企業外網路上，類似這樣需求的網路資料查詢下載服務，實不勝枚舉 。其中台灣省交通處港

灣技術研究所擁有的海氣象資料庫，由於其對於海域遊憩活 動的推廣、海洋資源的開發、航運與港灣建設、海岸環保或國防安全等乃爲一極有價 值之資料 [1]。因此發展一套夠支援網路資料安全查詢與傳輸的平台，對於港灣技術 研究所與參與此計畫的我們來說是一件相當重要的工作。

在本研究裡，爲了保持上述所提出的網路資料安全查詢與傳輸平台能爲網路使用 者所接受，我們乃選擇全球資訊網作爲主要架構。但是在網路資料的傳輸核心上，爲 了達成資料查詢與傳輸的安全性， push 模式 [2-6] 的資料傳輸架構是主要作法。有 關爲何選擇 push 模式作爲網路資料的傳輸核心，我們會於第二節中再詳加討論之。 本研究中所提出的架構基本上乃模仿電視傳送概念，網路使用者於獲得授權所需之資 料後，可透過 channel client －如同是一個頻道已經被設定好的電視機之前端程式 ，接收來自於 channel server（如同電視台一樣）的某固定頻道中之資料。由於 channel server 與 channel client 皆由本平台控制，兩者之間會經由認證協定以確 認身份。而爲避免資料於傳送過程中被擷取， channel server 與 channel client 間 會自動利用公開金匙法 (public key) 作爲資料傳輸時的保密機構 [7-8]。利用這個研究結果，我們並實做出港灣技術研究所海氣象資料庫網路查詢系統。而此 channel server 伺服器與 channel client 前端程式的研究成果，尚可運用於其他全球資訊網 上的新媒體資料傳送使用 [2-6]。其中目前最流行的線上軟體買賣，是一個可以直接 被應用的地方。

本論文主要由下列四節所構成。在第二節中，我們將探討爲何使用 push 模式來 做爲資料傳輸核心。而有關本平台的詳細系統架構則於第三節中描述之。第四節則爲 本研究之實做與結論。

2. 全球資訊網資料傳輸模式的探討

傳統上，全球資訊網是一種透過超鏈結 (hyperlink) 來連結資料的分散式多媒體 網路資訊系統。透過這樣的架構，使用者可以輕易的分享與取得所需資料。這種由使 用者上網自行瀏覽所需資訊的模式，我們可將之視爲是 Pull Model 的一個典範。所 謂的 Pull 模式就是指由系統產生特定的網頁 (homepage)，使用者必須主動進入此網 頁點選所需資料，因此主動權在於使用者端。當面對需要保證安全無疑的使用資料時， 在此種 Pull 模式的架構下，基本上最容易的作法就是利用存取管理來控制之。然而 當大量的資料（如海氣象資料等）要經過主管機管審核，同時只有部份資料可獲授權 時，最常被選擇的作法乃是利用 FTP 協定並透過適度之存取控制來提供使用者下載資 料。然而由於 FTP 的傳輸協定簡單，用 FTP 來做資料傳輸之最大問題乃在於系統安 全性的困難維護。爲求保障網路資料的安全性，未經許可之使用者不得自行上網擷取 資料。因此在保護系統安全的要求下，我們需爲每個資料需求者建立動態之特殊操作 環境以保障 FTP 傳輸。然而此種 Pull Model 的做法卻會造成另一項缺點，此缺點乃 在於當使用者擁有系統操作之主動權，從系統管理角度而言，如何正確維護系統整體 環境會是一件極爲繁瑣的事。

相較於 Pull 模式的做法，另外一種模式可被稱爲是 Push 模式。所謂的 Push 模 式做法，是指資料主動由伺服器端傳送至使用者端，伺服器端握有控制權。換句話說 在此模式下，使用者於選取所需資料並經許可確認後，資料會被主動根據安全需求傳 送給使用者。此種作法之好處乃在於：

（ 1 ） 系統安全容易維護，

（ 2 ） 資料易於保密，

（ 3 ） 使用者不需肩負系統操作難題。

傳統的全球資訊網架構，基本上原是一種 Pull 模式。然而隨著網站的多元化與快速 增加，爲了讓使用者免於自行上站尋找所需資訊， Push 模式作法的網站伺服器已逐 漸獲得網際網路使用者的青睞 [2-6]。此方面的發展，儼然已成爲全球資訊網上研 究的一個新方向。因此在本研究中，我們乃準備採用此種模式並加上安全的資料傳輸 控制來發展一個妥適的網路資料查詢與傳輸平台。

在資料傳輸的安全上，公開金匙法是本架構所採用的方法。公開金匙法與傳統的 編密技術最大的不同，即是它分別使用公開金匙與秘密金匙來做加密 (encryption) 及解密 (decryption) 的工作。傳統的編密技術（ 如 DES ）在加解密時，都採用同 一支密碼匙來運算，雖然速度上快很多，但在網路傳輸時卻有潛在的危險性。公開金 匙法就完全沒有這一層的顧慮，因爲加解密用的金匙是不一樣的。以目前的軟體技術 及硬體速度，利用公開金匙加密的時間已經可以接受。而即使利用超級電腦級的計算 機，卻很難在合理的時間內破解 1024 位元以上的秘密金匙。

3. 系統架構

在 Push 模式的架構之下，我們發展的 channel server/client 做法與電視機跟 電視台傳送資料的概念極爲類似。圖 3.1 是此平台的簡易系統架構說明圖。當網路使 用者先經由全球資訊網申請資料並於審核通過後，一個特定的 channel client 之前 端程式會被產生並自動經由 MIME 型態之電子郵件傳送給該使用者。由於此特製之 channel client 不會太大，同時內含資訊皆經適當編密，因此傳送過程不至造成任何 問題。當該 channel client 被執行後，就如同是一個頻道已經被設定好的電視機一 樣，一經啓動就只能接收來自於 channel server （如同電視台一樣）的某固定頻道。 由於 channel server 與 channel client 皆由系統控制，兩者之間會經由認證資料 以確認身分。

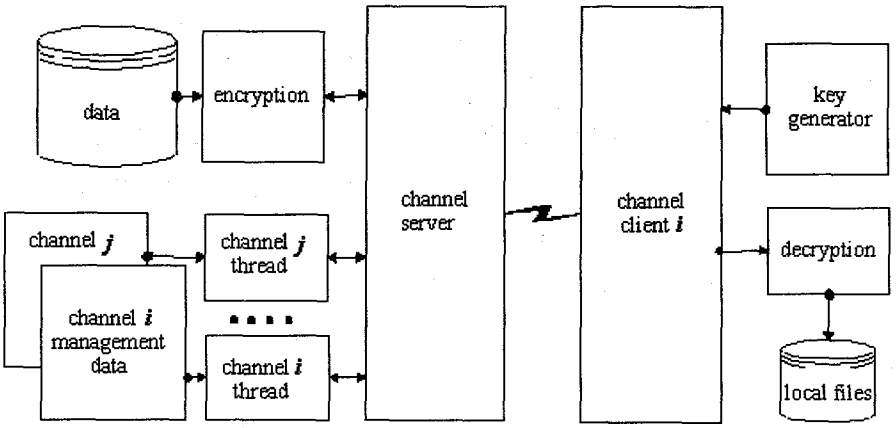

圖 3-1. Channel server/client 的系統架構圖。

其中這些資料包括有 channel client 的所在 IP 位址以及使用者帳號和密碼等。當 一切過程殊無疑義後， channel client 會根據所在電腦可用空間決定目前請求資料。 channel server 根據該使用者的申請之管理資料，通知 channel client 準備接收資 料之相關訊息。 channel client 此時乃會將自動產生的公開金匙傳送給 channel server。在經過適當確認後，該 channel client 的對應頻道會以所收到之公開金匙 編密申請資料並傳送給 channel client。由於只有 channel client 程式擁有對應之 秘密金匙，因此 channel client 可於收到編密資料後自行解密之。網路上的其他人 員即使獲得此資料，也無法知道資料內容。圖 3.2 是 channel server 與 channel client 間的傳輸協定範例。

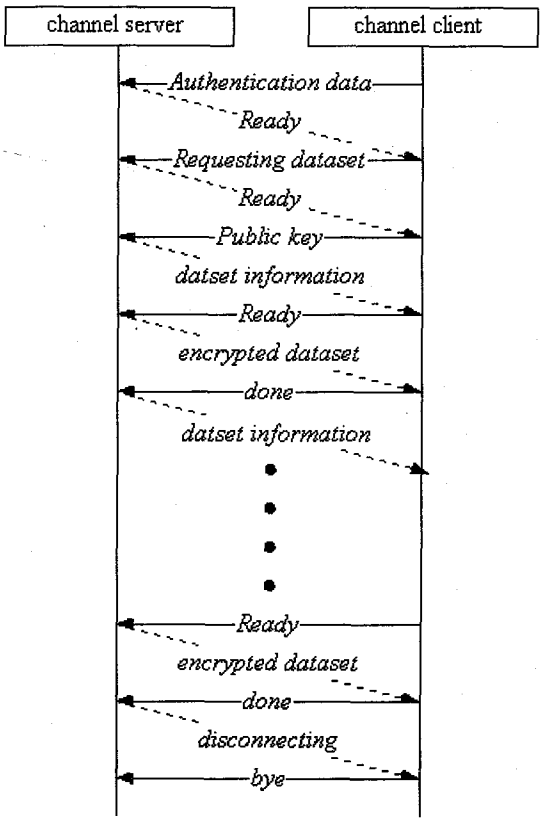

圖 3.2. channel server 與 channel client 間的傳輸協定範例。

4. 系統實做與結論

根據上節中的介紹，我們乃利用 Java 語言實際做出 channel server 與 channel client 。channel server 基本上是一個 multi-threaded 的伺服器。當每個 channel client 連上 server 時， server 會自動產生對應的 thread 來處理此頻道 的工作。在完成此平台後，我們更進一步利用這個架構發展出台灣省交通處港灣技術 研究所的海氣象網路資料查詢與下載系統。圖 4.1 則是它的系統架構圖。使用者首先 經由全球資訊網進入本系統，在經過查詢與選擇後，此資料請求會被自動轉成一個表 單並傳送給管理者。當管理者確定核准之資料內容後（通常是好幾百萬位元組）， channel server 會自動產生一個頻道與特製之 channel client 程式。而此 channel client 會被傳送給該資料申請者。由於本系統目前尚在測試階段，因此暫時 不對外界使用者開放。不過我們所發展的網路資料安全查詢與傳輸平台，其效果證實 確可達成預期目標。

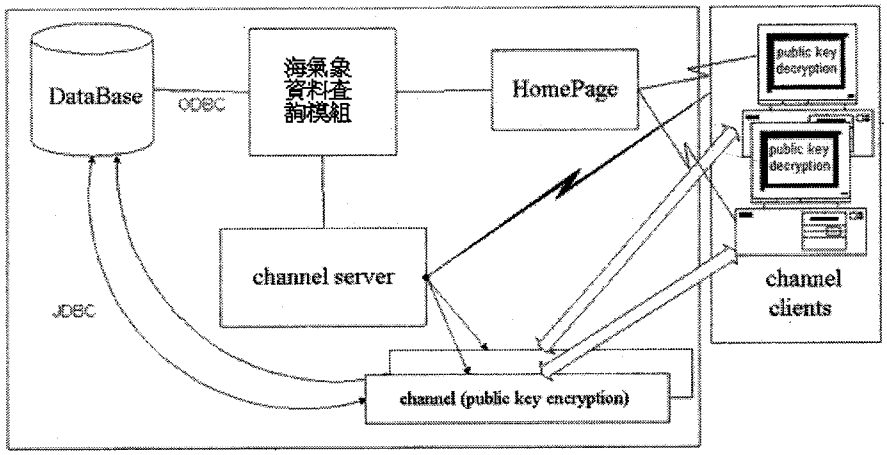

圖 4.1 港灣技術研究所之海氣象網路資料查詢與下載系統架構圖。

參考資料

[1] 簡仲璟、曾相茂，港灣海域海氣象特性研究-海氣象資料庫與查詢系統建立研 究，港灣技術研究所報告，台灣省政府交通處， 1996 。

[2] Castanet, http://www.marimba.com/。

[3] BackWeb, http://www.backweb.com/。

[4] Arrive, http://www.arrive.com/。

[5] PointCast, http://pioneer.pointcast.com/ 。

[6] Netcaster, http://home.netscape.com/。

[7] William Stallings ， Network and Internetwork Security Principles and Pactice 。

[8] RSA Data Security, Inc.， http://www.rsa.com/。