一個資料異動檢核自動化系統之實作

An Implementation of Automatic Checking System

謝濱燦　　莊韋軒
德明財經科技大學　　德明財經科技大學
資管管理系　　資管管理系
助理教授　　學生
bintsan@takming.edu.tw　William101323@gmail.com

摘要

因網際網路全球化使消費者空間不限於企業本地與國籍，連時間也沒有白晝與黑夜之分，企業的營運進入了全年無休的不停機時代。企業的營運特性產生變化，但是企業的營運時間卻因為人力成本結構的問題無法對應變成全年無休的人員輪班的型態，企業擁有二十四小時的商機，卻無法提供全年無休的人員服務。金融業需以資訊技術提供全天自動化又安全的服務，解決人力問題並提供升客戶的信賴。本論文主要探討利用程式分析檔案資料異動的情況，以主從式(Client/Server)架構定時監控數百台的伺服器,並針對任何檔案的新增、刪除、修改即時寄發電子郵件通知管理者, 有效簡化網管人員的維護人力。

關鍵詞:自動化、分析

ABSTRACT

The globalizaction through internet has made the customers worldwide get beyond the limit of time and space. It makes no difference between local enterprises and international ones, as well as day time and night time. The features of enterprise operations vary substantially whereas the operating hours cannot open all year round due to the obstruction of labor cost. Enterprises gain commercial opportunities anytime and anywhere while the uninterruptible service cannot be provided. For financial service industry, the automatic service whenever necessary should be provided by informational technique so as to solve the problem of human resource and increase customer reliability. This research probes into the condition of information variation through program analysis. With the utilization of Client-Sever Architecture, a host server manages thousands of client servers simultaneously. Therefore, as soon as any files are added, deleted, or revised, the manager would be notified by email promptly, which efficiently streamlines the manpower of administrators.

1. 研究動機

企業經過多年的資訊化後，企業運作大部分與資訊系統早合為一體，密不可分，傳統的資訊系統導入的主因，早期多半是希望能夠將許多紙本記錄的工作項目或內容，透過資訊技術予以儲存與傳播，將企業的運作與邏輯透過實作資訊系統方式，整合到企業之中。企業導入資訊化，大幅縮減以前人工的問題，以前人工的方式輸入資料一來有錯誤，二來檢查方式比較不人道，花費大量的人力與時間，導入後大量縮短的時間，可以保存更多的系統資訊或資料，以便日後有更多元的運用。

2. 研究目的

公司資訊系統規模龐大，基本上可分為前中後台，開發人員隨著系統的數量與功能的增加，分工也越分越細。而當系統發生問題時，系統管理人員總是花費許多時間查找問題。原因在於新系統管理人員不太了解系統的架構與資料流，往往也沒有文件可以參考。除了新問題，舊有的系統也常常出問題，好不容易找出問題點，請開發人員修正舊有問題，但是公司又希望開發人員能優先開發新功能，使開發人員沒有多餘時間修正舊系統或常常隨意修改便上線了事。

如何在短時間內針對數百個交易系統有效的監控,迅速掌握哪支程式被修改、刪除、新增並即時通知網管人員，便成為十分重要的議題。若能即時掌握，便可更快排除交易系統的異常及不穩定。

3. 研究方法

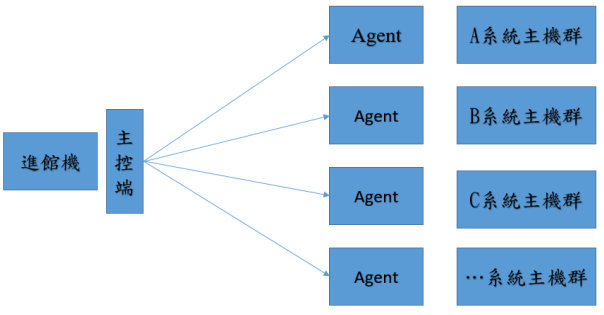

圖10 自動化分析程式架構

如圖 10，本研究的自動化分析程式架構，使用此方法來解決本公司長久以來的痛,花費大量的人力與時間。使用此方法可以得到大量的改善，解決人力與時間不足的問題，不管是程式人員的異動或者駭客入侵竄改程式，可以在短時間內就可得知結果，分成兩個部分進行，一個是有管理介面的主控端，另一個是 Agent 端，由主控端發起派送 Agent 到各系統主機群中，我們定義好時間，時間到就會開始運作，將我們所需的資料送回主控端這邊,主控端會自動進行比對的機制,檢核到異常,立即發送 Mail 至公司電腦或個人手機上，以利於優先處裡的事件。

本研究使用HMAC的完整性檢查，當一個檔案或訊息自遠端傳來,即可利用赫序函數來確其正確性,傳送的一方需要利用金鑰對訊息計算認證碼(MAC)傳送時將訊息及MAC交給收方，收方拿出自己的金鑰，對於所收到的訊息訊算訊息認證碼(MAC)再將自己計MAC與對方送來的MAC進行比較，若相同則確認訊息無誤。

4. 本研究之創見

Agent 端

主要布置於系統主機上，負責定時檢核，監控系統上的檔案，其流程及功能如圖 11 所示，各模組功能分析如下。

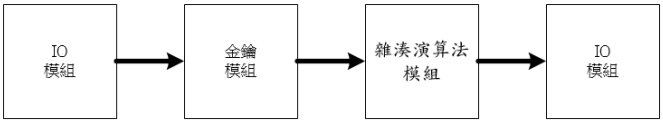

圖 11 Agent 端模組功能

IO 模組:我們將定義好的程式路徑，會讀一筆後，接由金鑰模組處理。

金鑰模組:確保資料的安全性，在計算中加入密碼。

雜湊演算法模組:定義好的程式路徑和 Key 計算,將計算完的結果分成路徑和程式。

IO 模組: 將程式路徑和 Mac 值寫入檔案，這個檔案會自動寫回主控端的主機上。

主控端

主要放置於進館機，負責派送 Agent 及接收 Agent 回傳的資訊並進行檢，一旦發生任何異動包括新增、刪除、修改等均會寄發 Email 給管理者,核圖 12 所示，各模組功能分析如下。

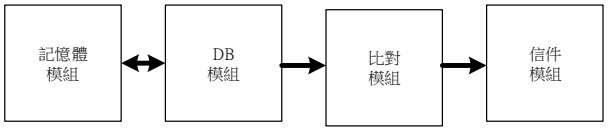

圖 12 主控端模組功能

記憶體模組:這邊會把 DB 的資料全部讀到記憶體裡面，例如說某套系統的程式路徑與計算完的 Mac，以利於增加比對速度。

比對模組:Agent 端回傳的檔案跟記憶體中的資料作比對，有相同的路徑和程式代表沒有被修改，如果比對出來是新增、修改、刪除，以上的其中一種，就代表有人異動程式。

信件模組:這邊將比對模組的結果有異動的部分,就會立即寄送Mail,相對應的系統人員就會收到這封MAil,就會清楚自己的系統是否被人異動或者被駭客入侵串改資料，提早預警的作用。

5. 相關技術

5.1. 赫序函數與訊息認證碼

赫序函數(Hash Function)主要應用於檔案或訊息的完整性檢查,當一個檔案或訊息自遠端傳來,即可利用赫序函數來確其正確性。收到的一方針對該訊息計算其赫序值，再將所算出來的赫序值與送方所公告的赫序值相比較,若相同則確認訊息無誤,反之則應重新傳送。常見的赫序函數包括 MD5,SHA-1。赫序函數適用的情境為一對多，例如報稅軟體的下載，可置於官網供多位民眾下載，民眾下載後再計算軟體的赫序值並與官網公告的赫序值比較。[3]有別於赫序函數適用於一對多,訊息認證碼(MAC)適用於任意兩個實體傳遞資訊。MAC 的使用前提是該兩實體需要事先共享一相同的金鑰。

如圖 1 所示, 傳送的一方需要利用金鑰對訊息計算認證碼 MAC,傳送時將訊息及 MAC 交給收方,收方拿出自己的金鑰，對於所收到的訊息訊算訊息認證碼 MAC，再將自己計算的 MAC 與對方送來的 MAC 進行比較, 若相同則確認訊息無誤。

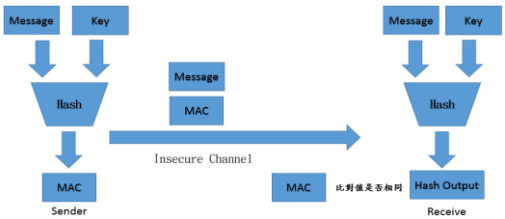

圖 1 HMAC 運作程序

5.2 異質資訊系統之自動化警示機制之研究

李建弘於2006 [1]提出一使用直譯語言的技術與資料流程導向的觀念為警示系統建立開放性的標準介面，以系統整合的方式自動化警示機制功能，並實作雛型系統來驗證研究的可行性，希望能透過研究成果來替企業提供一個自動化的整合警示功能，並為企業創造更大的效益。

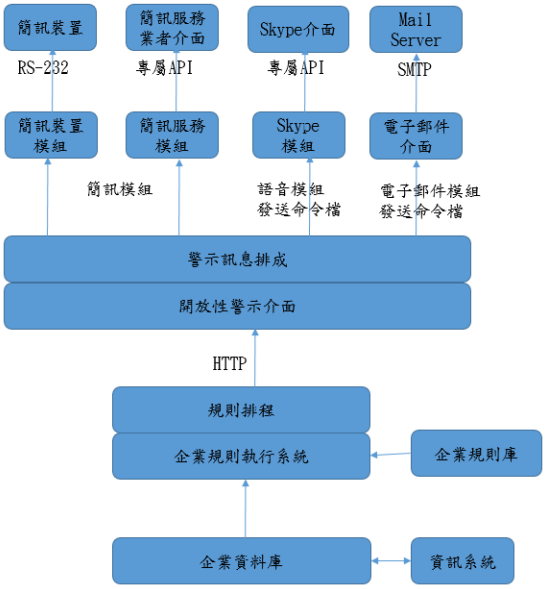

圖2 異質資訊系統警示機制整合架構

如圖2,將每一個不同的系統模組獨立出來，並且統一不同系統模組之間的驅動介面標準化，並將行動警示訊息發送裝置元件化，可以讓中小企業到中大型企業都可以使用整個自動化警示裝置的效益。運用以上的觀念與研究前提，整個研究動機便專注在異質的企業資訊系統下，以流程的觀點來建立警示功能的機制，並不需要大幅度對個別資訊系統修改或重建，而且可以延伸整體的機制，在流程或決策關鍵點之中，可以主動透過行動警示的裝置，即時警示相關人員，讓整個企業不會因原有系統架構的等待問題產生缺失。

如圖3與圖4，此研究以學生點名系統之缺課警示機制為例來對整個警示系統的運作進行模擬示範。對於學生的家長卻呈現一個事實，那就是發現已經無法挽回的成績單，甚至產生許多不必要的糾紛。若能在學生缺課時能即時的通知家長，讓家長知道情形並馬上處理，就可讓整件事情得到更好的結果。

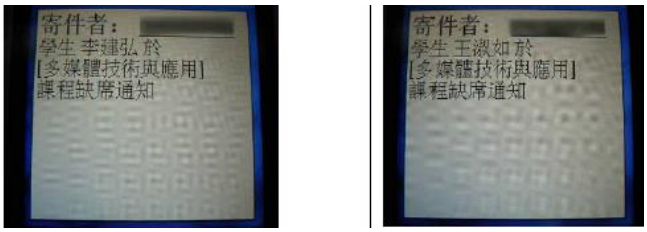

圖3 簡訊範例畫面

圖4 Skype警示訊息外撥畫面

5.3遠端伺服器監控管理系統設計與實作

蕭富方於2006 [2]提出-遠端伺服器監控管理系統，讓系統管理人員可以遠端監控伺服器，隨時掌握被監控端伺服器的狀況。若伺服器發生異常狀況，系統管理人員能夠立刻發現，立即採取相對應的應變措施，以應變突發之異常狀況。為了讓系統管理人員可以更方便管理伺服器，該研究設計系統之自動控管功能，在伺服器發生異常情況時，為了維持伺服器之正常運作，做出相對應的應變措施，系統將自動處理異常狀況。目前多數的伺服器管理系統，較不強調系統控與硬體控制之結合，若加強系統管理與硬體控制，整合伺服器管理和硬體控制機制，以提升伺服器的整體效能運作，達到系統自動微調和硬體自動微調之功能，便能使系統與硬體更有效率，達到最佳化之管理目的。

該研究以以Fail－Over 為例，透過網路監視系統狀態與硬體狀態下達指令操作，使用IPMItool 對被監控端伺服器下達操控指令，實現遠端操作之目的。

1. 查詢被監控端伺服器的電源狀態（如圖5）查詢被監控端伺服器，該台主機的電源狀態。

2. 遠端關機(如圖6)遠端關閉被監控端伺服器電源。再下達查詢電源狀態之指令，檢查電源狀態是否被更改。

3. 遠端開機(如圖7)遠端開啟被監控端伺服器電源。再下達查詢電源狀態之指令，檢查電源狀態是否被更改。

4. 獲取 CPU 溫度（如圖8）顯示 CPU 溫度及其狀態是否為正常。

```
#ipmitool -I lan -H 192.168.16.5 chassis power status
Chassis Power is on
```

圖5 指令操作－查詢電腦的電源狀態

```
#ipmitool -I lan -H 192.168.16.5 chassis power off
Chassis Power Control: Down/Off

#ipmitool -I lan -H 192.168.16.5 chassis power status
Chassis Power is off
```

圖6 指令操作－下達關機指令

```
#ipmitool -I lan -H 192.168.16.5 chassis power on
Chassis Power Control: Up/On

#ipmitool -I lan -H 192.168.16.5 chassis power status
Chassis Power is on
```

圖7 指令操作－下達開機指令

```
Locating sersor record...
Sensor ID              : Processor 1 Temp (0x31)
Sensor Type (Analog)   : Temperature
Sensor Reading         : 32 (+/ - 6) degrees C
Status                 : ok
Lower Non-Recoverable  : na
Lower Critical         : 8.000
Lower Non-Critical     : 15.000
Upper Non-Critical     : 58.000
Upper Critical         : 68.000
Upper Non-Recoverable  : na
```

圖8 指令操作－獲得CPU的溫度

圖9 偵測被監控端伺服器系統資訊之輸出畫面

中央管理伺服器透過 Out-of-Band 的方式，遠端開啟另一台被監控端伺服器，使用Fail-Over 的機制，將原本的網路流量導向另一台可用的伺服器，以維持網路對外連線的正常運作，另一台被監控端伺服器的系統資訊如圖9 所示。

6. 系統實作成果

因系統環境十分複雜，線上主機約略 800 台左右，在如此龐大主機數量下，如何有效的檢核程式就十份重要，因人工檢核浪費大量人力而且又沒有準確性，如

果可以使用自動化的方式來檢核這塊，所需要的時間就會快速許多，但並非速度快就好，還需要準確性非常高的驗證，本研究使用 HMAC 的方式來處理。如圖 13 所示，這個部分是主控端的派送、主機的名單建制以及最重要的比對機制都在主控端。

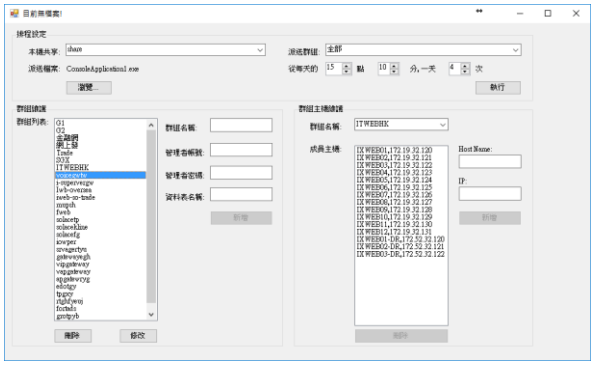

圖 13 自動化程式比對主控端

本研究抽取 20 個系統進行比對測試，每個系統的主機數量均在 2~5 台，有少部分系統主機數量有 10~12 台，這 20 個系統當中，每一個系統的性質均不同，所以在程式的數量上不會一樣，每個系統均都測試 10 次以上平均出來整理如表 1 所示。

名稱	間（秒）	數(台)	數量	名稱	間（秒）	數(台)	數量
BUJOPWAZXCSDV	0.8	4856	2 台	ISSXSRB	0.01	1001	4 台
Capital	12	67112	5 台	IXWEB	0.01	101	10 台
capitalfutures	0.23	1345	5 台	MOBAPP	0.01	1112	12 台
CXS	0.45	2001	2 台	OIEGJKV	0.1	3003	5 台
EIORYKSJNVSDV	0.2	701	2 台	QKLSKERMOPRE	0.03	501	4 台
EXTRAXDE	0.1	301	2 台	QWDFGRTY	0.01	91	4 台
FBGHWEFWEF	0.07	2001	3 台	STOCXKEARY	0.01	101	2 台
fund	0.02	1001	5 台	SXVGATEXAYG	0.01	101	2 台
GXASERTY	0.01	401	4 台	VXOICTEW	0.01	101	12 台
HISTGYA	0.01	91	4 台	WUQWJKV	0.01	31	10 台

表 1 系統比對花費時間統計

經由本研究的比對方法，主機的程式數量上越多，計算時間也就越久，但程式數量在 1 萬以內的平均若在 1 秒內，很明顯的跟之前的人工檢核上，速度上快許多準確性高，因系統管理人員不可能常常都在電腦前面，但唯獨手機一定會在身邊，所以我們整合可以讓手機收到 Mail，增加讓管理人員處理的時間，如圖 14 顯示 WahyLoad9999.aspx 為新增之檔案。

圖 14 手機收到 Mail 程式異動

系統	計算時	程式之	系統	系統	計算時	程式之	系統

7. 結論與建議

本研究所提出程式自動化分析判斷，可應於當前程式上線的平台，大幅縮短人力和時間，在短時間內可以得知線上主機程式是否有被程式人員修改，提早做準備。本研究驗證，以前6萬7千多筆程式人工檢合需花3小時間，現在只要需花1分鐘時間，整個大幅度縮短了180倍的時間與人力,如果一天要比多次的話,人工檢核根本來不及，使用本研究的比對方法，可以達到一天多次的比對，在短時間內就可以得知重要的訊息，希望解決人力問題並提升客戶的信賴。

參考文獻:

[1]李建弘,2006,異質資訊系統之自動化警示機制之研究,靜宜大學，資訊管理研究所, 碩士論文。
P28,2.1~2.1.1，P28,2.1.2，P86-P97
[2]蕭富方，2006,遠端伺服器監控管理系統設計與實作,世新大學，資訊管理學系, 碩士論文。
[3]資訊與網路安全技術(第二版),1-11頁， 6-6~6-10頁。