應用安全設計樣式分析與設計物聯網系統

劉博仁 李文廷* 郭家旭
國立高雄師範大學軟體工程系

Po-Jen Law, Wen-Tin Lee*, Chia-Hsu Kuo
Department of Software Engineering,
National Kaohsiung Normal University

Email: lawpojen.1992@hotmail.com, wtlee@nknu.edu.tw, kuoch@nknu.edu.tw

摘 要

近幾年物聯網越來越流行，許多的資訊服務也漸漸的與網路結合。然而，物聯網裝置之間在傳輸溝通上缺少了安全性，可輕易攔截裝置間傳遞的訊息，進行訊息修改或發動攻擊。因此，為了解決這樣的問題，本研究針對系統安全性採用系統分析與設計流程。在需求分析階段，分析使用案例圖及系統活動圖以了解系統需求。進一步根據使用案例圖、情節及活動圖建立系統的初始架構。在系統設計階段，在系統架構中針對物聯網裝置間的通訊過程使用五個安全性設計樣式希望可以強化其安全性，進一步完成系統元件與類別的細部設計。

關鍵字: 物聯網、安全設計樣式、安全性系統分析與設計

一、緒論

物聯網(Internet of Things, IoT)是資訊與通訊科技中一個熱門的話題。物聯網顧名思義就是把一個物體加上 RFID、無線通訊等技術，讓該物品可以跟電腦、手機或物體進行通訊溝通。由此，建構了一個可以覆蓋全世界萬事萬物的物聯網[1]。

至今預計全球已有 50 億台裝置連線到網路上，且到了 2020 年連線上網的裝置預計將會到達 250 億之多。[2] 近幾年物聯網越來越流行，許多的資訊服務也漸漸的與網路結合。在未來物聯網將成為主流，不論是哪個領域都有可能將導入物聯網，如：醫療器材、教學器材等。然而物聯網是世界中，物體與物體之間進行通訊溝通，溝通的過程中相對的安全性的問題將就此產生。例如透過網路來操控澆水系統，這個系統缺少了(1)未加密的應用程式資料(2)未加密的無線通訊(3)未加密的敏感的使用者信息。[3] 即使今天我們的科技發達，但還是有許多具有實體裝置在互相進行資料傳輸進行溝通的時候是在沒有加密環境下進行的 。

因此，本研究將以建置一個系統為例並針對其中所裝置間溝通的時候碰到的安全性問題套用五個設計樣式，希望能改善現在遇到的安全性問題。本研究的重點將著重於裝置間通訊時候的安全性問題並針對該問題套用安全性設計樣式以確保裝置間的通訊的安全性。第三章主要是介紹本研究所建制之系統架構，並說明系統流程。第四章說明本系統透過軟體工程之方法來進行系統分析。第五章說明本研究所套用的設計樣式之循序圖及設計樣式流程。第六章則是相關研究論文的簡介。第七章將明確列出本研究之貢獻。

二、背景知識

本論文之實作系統背景知識分為無線射頻辨識(Radio Frequency Identification , RFID)、藍牙通訊技術及 Arduino 及安全性設計樣式，分別說明如下：

2.1 RFID (Radio Frequency Identification)[8,9]

RFID 是一種透過無線電訊號辨識特定目標並讀寫相關數據的一種無線通訊技術。我們在物體上貼上數據標籤，以自動辨識與追踪該物品。 本研究系統裡主要是運用 RFID 的標籤卡片，來進行本系統之使用者的辨識。當使用者將 RFID 卡片放到 RFID Reader 前 Reader 會讀取卡片的 ID 資訊，回傳給 Server 判斷是否有這位使用者。

2.2 藍牙通訊技術[10][11]

藍牙是一種無線通訊技術，它讓裝置之間可以在短距離間做資料的交換。生活中許多電腦裝置都可以看到藍牙的身影，如手機、平板和印表機等等。本系統將藍牙運用在腦波裝置上，腦波裝置透過藍牙將偵測到的腦波資料傳送到 Server 上，讓 Server 能夠針對這些資料做跟進一步的處理。

2.3 Arduino[4]

Arduino 是一個開源的單晶片控制器，它採用了開源的軟硬體平台，建構出一個簡易的 I/O 介面板，並使用類似 Java、C 語言的 Processing/Wiring 開發環境。[4]本研究的系統感測器及 RFID Reader 都是透過 Arduino 來建置並實踐 IoT。

2.4 安全性設計樣式[5, 7]

安全性設計樣式是一種為了解決系統安全性所產生的設計樣式，它包含許多專家在解決安全性問題這方面的知識，並且提供可重複使用的架構和方法幫助程式設計師解決系統安全方面的設計。本研究所套用的五個安全性設計樣式(Security Design Pattern)：

- Secure Logger Pattern[5,7,12]
- Secure Directory Pattern[5,7]
- Error Detection and Correction Pattern[5,13]
- Exception Manager Pattern[5,7]
- Input Validation Pattern[5,7]

三、系統簡介

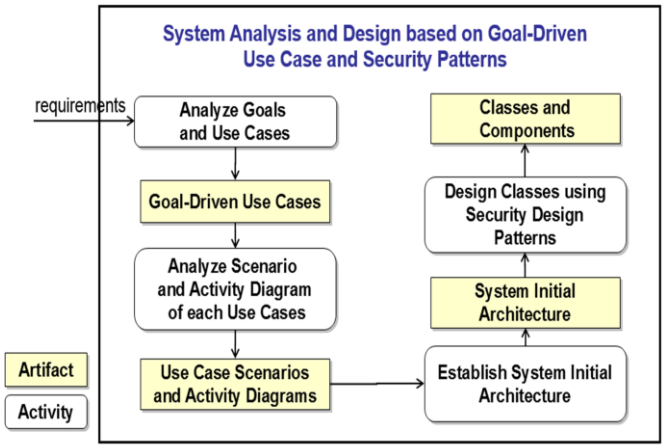

圖 1、系統分析與設計流程

本研究開發之系統將 RFID 卡片透過讀卡機進行身份辨識後，進行室內的感測器進行當前的室內環境情況，並將偵測到的環境資訊發送到使用者手機上告知使用者。

首先，在第一步驟針對系統需求制定目標與使用案例，產生目標驅動使用案例。在第二步驟分析使用案例圖中各個使用案例之情節及系統使用步驟，並產生系統活動圖。第三步驟根據使用案例圖、情節及活動圖建立系統的初始架構。最後第四步驟，在原有的架構中加上安全性樣式設計，完成系統元件與類別的設計。

圖 2 為本研究之架構及運作流程。步驟一，使用者必須將使用者擁有的 RFID 卡片靠近讀卡機。步驟二，當讀卡機讀到卡片後會將讀到的卡片資料送給伺服器進行身份確認。步驟三，伺服器確認身份無誤後就會發送開門指令到控管門鎖的裝置，把門打開。步驟四，收到開門指令的同時，裝置會啟動室內的所有環境感測器，針對室內的環境進行偵測。步驟五，偵測完成後，收集所有偵測到的資料。步驟六，資料收集完成後回傳資料到伺服器。步驟七，開門同時伺服器會透過藍牙搜尋腦波裝置，若有跟腦波裝置連線成功，則開始收集腦波偵測到的使用者情緒之相關資料。步驟八，腦波裝置回傳腦波資料給伺服器，伺服器分析完使用者情緒後會根據其分析結果歸類出使用者是生氣還是快樂，在啟動相關類型的音樂。步驟九，伺服器根據使用者設定好的雲端服務，對其進行連線。步驟十，將環境資料跟雲端資料一起發送到使用者手機上。步驟十一，使用者修改雲端服務等相關設定時，應用程式會回傳使用者修改的設定資訊。

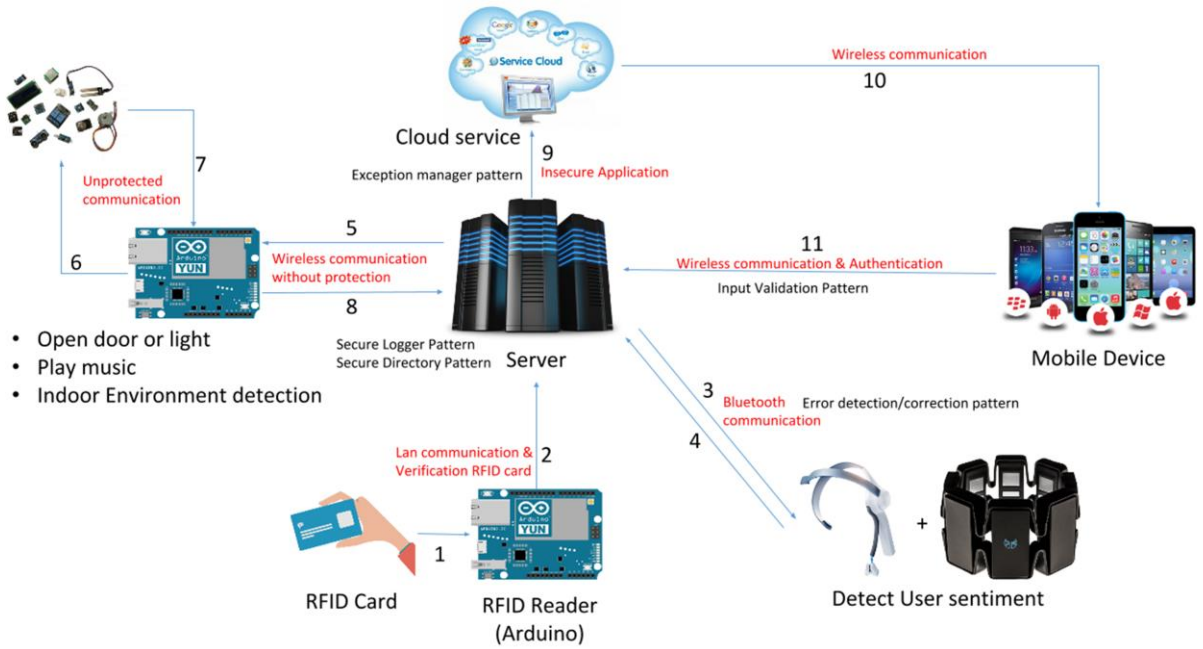

圖 2. 系統架構及運作流程

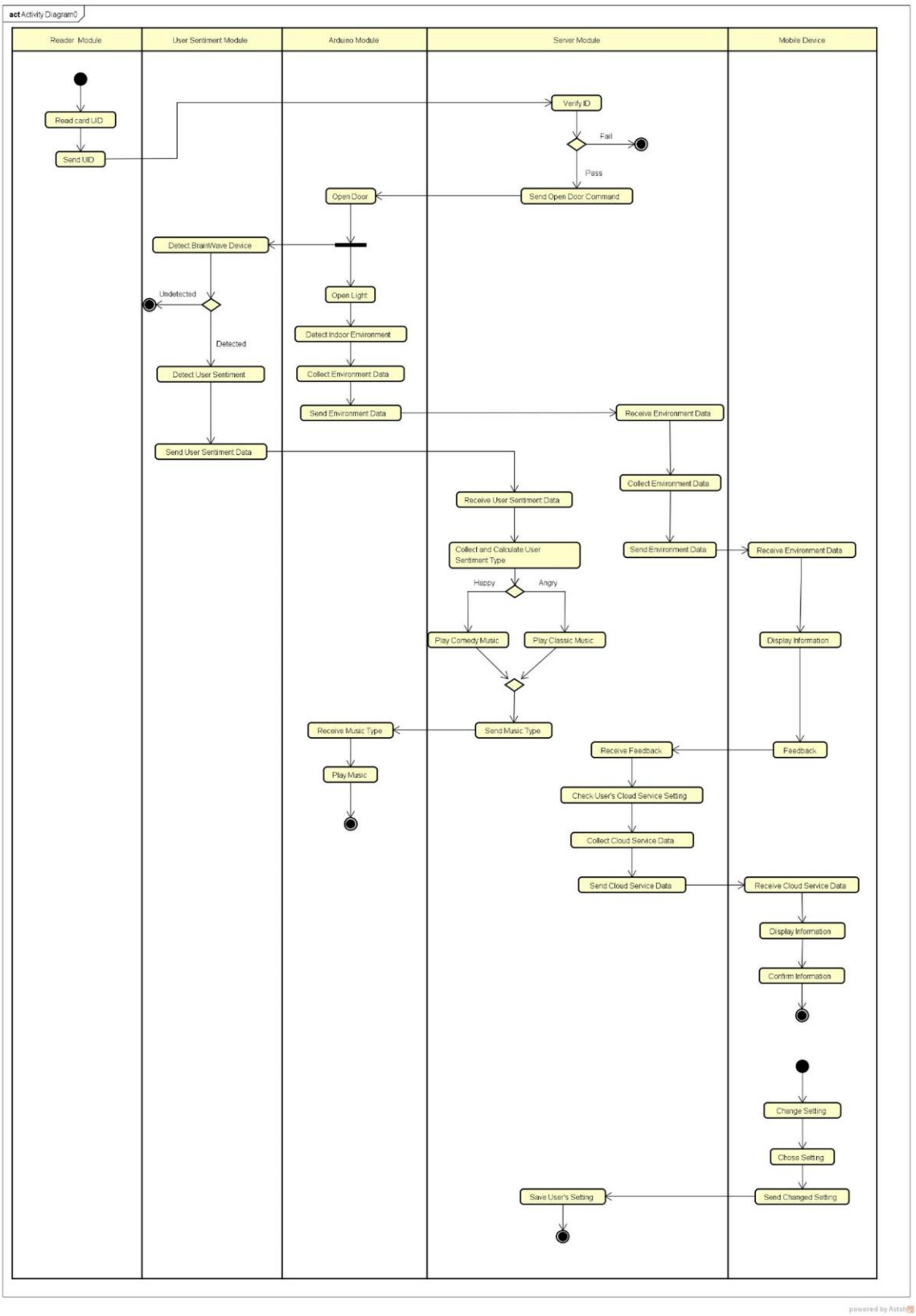
act Activity Diagram0
Reader Module
User Sentiment Module
Arduino Module
Server Module
Mobile Device
Read card UID
Send UID
Verify ID
Fail
Pass
Send Open Door Command
Open Door
Detect BrainWave Device
Undetected
Detected
Open Light
Detect Indoor Environment
Collect Environment Data
Send Environment Data
Receive Environment Data
Detect User Sentiment
Send User Sentiment Data
Collect Environment Data
Receive User Sentiment Data
Collect and Calculate User Sentiment Type
Send Environment Data
Receive Environment Data
Happy
Angry
Play Comedy Music
Play Classic Music
Display Information
Receive Music Type
Send Music Type
Receive Feedback
Feedback
Play Music
Check User's Cloud Service Setting
Collect Cloud Service Data
Send Cloud Service Data
Receive Cloud Service Data
Display Information
Confirm Information
Change Setting
Chose Setting
Save User's Setting
Send Changed Setting

圖 3、系統活動圖

圖 3 為本研究系統活動圖，圖中顯示了本系統更加詳細的流程。圖 2 為本研究之系統中裝置間相互溝通的連線方法及每一個溝通所套用之安全性設計樣式。圖 2 中 RFID Reader 是透過有線的連線方式來與伺服器做資料傳輸。本系統中所有感測器、門鎖、音樂播放裝置及使用者手機都是透過無線的連線方式來與伺服器溝通。在這樣的連線環境下，每一個連線方式都有潛在的安全性問題。在圖 3 中伺服器端會紀錄所有伺服器上所執行過的動作，因此我們需要有針對紀錄(Log)的安全性設計。另外，使用者手機發給伺服器訊息，本系統將套用 Input Validation Pattern 來驗證使用者所有的輸入是否正確及安全。圖中 Unprotected communication 的部分則是基於硬體間溝通的安全性問題，例如讀取 RFID 卡片資料的時候或是汽車遙控器發出訊號的時候，透過訊號截取器或許可以完整截取到所發出的訊號.。針對圖 2 的安全性問題本研究將著重於以下五個安全性設計樣式 (Security Design Pattern)：

- Secure Logger Pattern
- Secure Directory Pattern
- Error Detection and Correction Pattern
- Exception Manager Pattern
- Input Validation Pattern

四、需求分析

在系統需求分析中針對活動圖及使用案例圖進行分析，使用案例圖的分析結果如圖 4。圖 4 中使用者會用到的功能主要有雲端服務通知、播放音樂、驗證 RFID 身份及使用者情緒偵測。使用者在完成 RFID 驗證後，系統會將門鎖打開讓使用者進入室內。若室內太暗的時候系統會自動將燈打開。在雲端服務通知的部分，目前本系統是以 Google 日曆為例。關於播放音樂的部分則是，當裝置接收到伺服器的播放音樂指令後便會開始播放音樂。環境感測的部分則會是啟動所有在線的感測裝置來對環境進行感測。

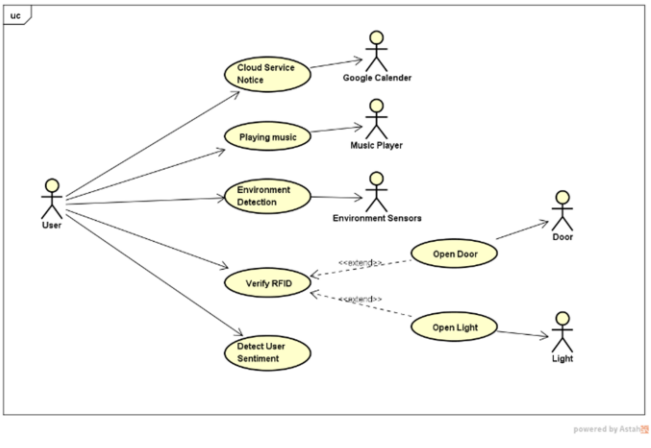

圖 4、系統使用案例圖

圖 3 為系統活動圖，各活動之細節說明如下：

Name	Activity
Read Card UID	讀取使用者的 RFID 卡片中的 ID 資訊。
Send UID	將讀取到的卡片 ID 資訊回傳給伺服器
Verify ID	收到卡片 ID 資訊並進行 ID 驗證
Send Open Door Command	發送開門指令
Open Door	收到開門指令後將門鎖開啟
Detect BrainWave Device	偵測使用者是否有沒有佩戴腦波裝置
Detect User Sentiment	偵測使用者當下的情緒
Send User Sentiment Data	將使用者情緒資料回傳給伺服器
Open Light	開啟室內燈光
Detect Indoor Enviroment	偵測室內環境
Send Environment Data	將環境資訊回傳給伺服器
Receive User Sentiment Data	接收使用者情緒資料
Collect and Calculate User Sentiment Type	收集並計算使用者情緒
Play Comedy Music	播放有趣的音樂
Play Classic Music	播放古典音樂
Send Music Type	發送要播放的音樂類型
Receive Music Type	接收要播放的音樂類型
Play Music	開始播放音樂
Receive Environment Data	接收環境資訊
Display Information	將環境資訊顯示給使用者看
Feedback	使用者回傳訊息給伺服器
Receive Feedback	接收使用者回傳資訊
Check User's Cloud Service Setting	檢查使用者雲端服務設定
Collect Cloud Service Data	收集雲端服務資訊
Send Cloud Service Data	發送雲端服務資訊
Receive Cloud Service Data	使用者端接收雲端服務

	資訊
Display Information	顯示雲端服務資訊
Confirm Information	確認所顯示的服務資訊
Change Setting	使用者更改雲端服務
Chose Setting	選擇雲端服務
Send Changed Setting	設定修改後將修改資訊發送給伺服器
Save User's Setting	接收修改設定資訊 並儲存使用者設定

五、系統設計

本研究針對系統所套用的五個 Security Design Pattern 的循序圖與類別圖分析和安全性問題進行分析。接下來將個別說明本論文中所套用的五個 Security Design Pattern，以下是這五個 Pattern 的循序圖與類別圖說明：

I. Secure Logger Pattern：

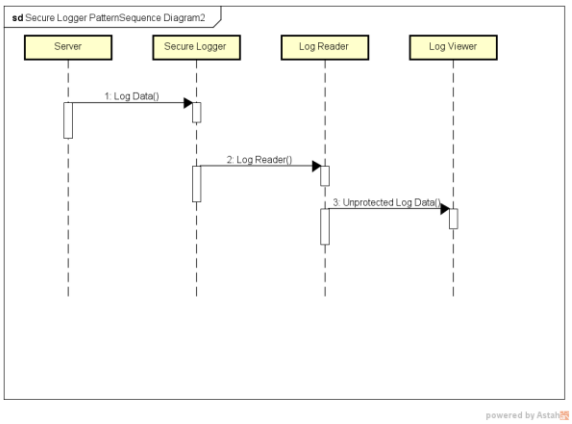

圖 5、Secure Logger Pattern 之循序圖

圖 5 是系統中套用的 Secure Logger Pattern 的循序圖。Server 會將所有的 log 資料都傳給 Secure Logger 將資料進行加密並儲存起來。當管理員需要調閱 Log 的時候 Log Reader 會從 Secure Logger 調出資料並將資料解密，在把解密後的資料傳給 Log Viewer 讓管理員查閱。

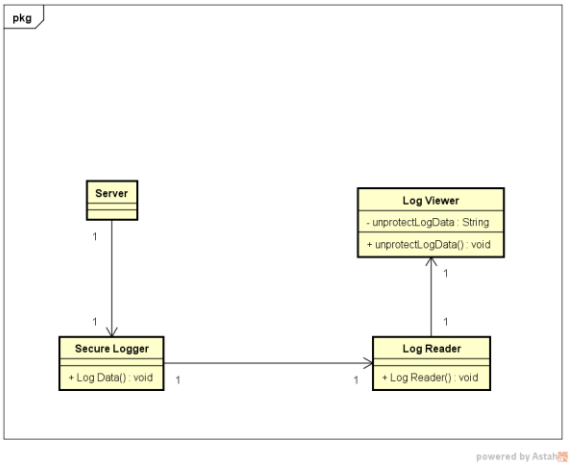

圖 6、Secure Logger Pattern 類別圖

在 Server 上我們會有許多要處理的任務，每一個 Server 的動作都會需要被記錄下來。因此，在 Server 裡面可以看到我們有許多的類別，Server 在處理任務的同時會將每一個動作傳給 Secure Logger 記錄下來。Log Reader 的部分是負責在管理員需要調閱記錄的時候會跟 Secure Logger 去撈記錄。最後透過 Log Viewer 來呈現所得到的資料給管理員。

II. Secure Directory Pattern ：

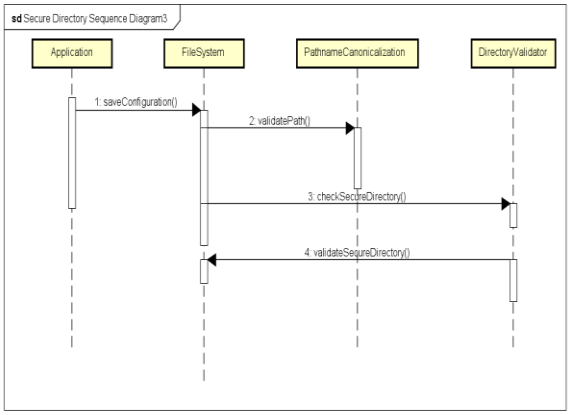

圖 7、Secure Directory Pattern 之循序圖

圖 7 中說明了當 File System 接收到使用者手機端傳來的使用者設定變更。File System 會去驗證使用者輸入是否安全及存入資料的路徑。

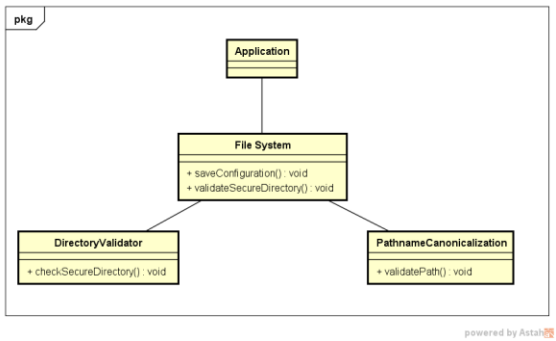

圖 8、Secure Directory Pattern 類別圖

Secure Directory Pattern 裡面的 Application 是負責將使用者的所有輸入來傳給其他的類別去做處理。DirectoryValidator 跟 PathnameCanonicallzation 的部分是在驗證使用者的輸入，File System 的部分是驗證通過後將會處理使用者的輸入。

III. Error Detection and Correction Pattern：

這個設計樣式的部分主要是套用在 Server 跟使用者所佩戴的腦波裝置做溝通連線上。當使用者開門後，Server 會自動嘗試的跟腦波裝置做連線。當連線成功，Server 會不斷的接收腦波裝置所偵測到的腦波資料。若發現腦波資料發送不正常或無法預期的錯誤時，Server 透過這個設計樣式來嘗試的修正該資料。

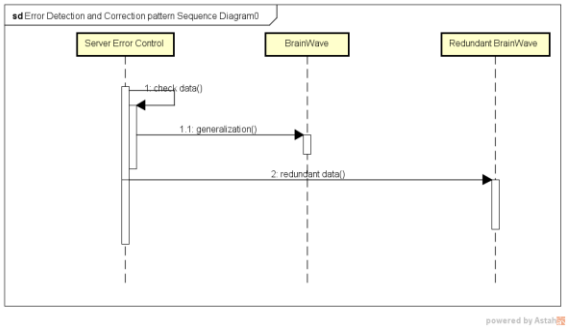

圖 9、Error Detection and Correction Pattern 之循序圖

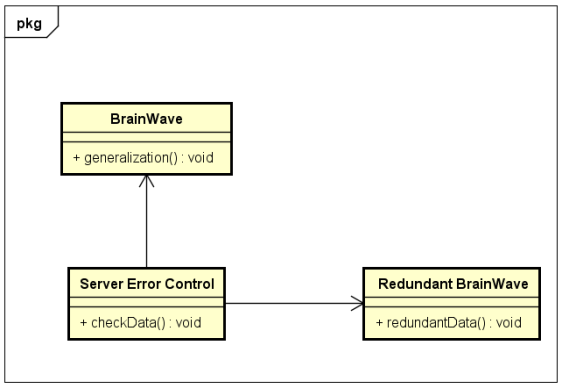

圖 10、Error Detection and Correction Pattern 類別圖

這部分是被套用到 Server 與腦波裝置通訊上。腦波會不斷的將偵測到的資訊傳給 Server。萬一再傳送的過程中發生了錯誤，就會由 Server Error Control 來處理任何的錯誤信息，在這邊我們假設腦波會發送我們不會用到的其他資訊。因此在這裡加入了 Redundant BrainWave 的類別來處理多出來的信息。

IV. Exception Manager Pattern：

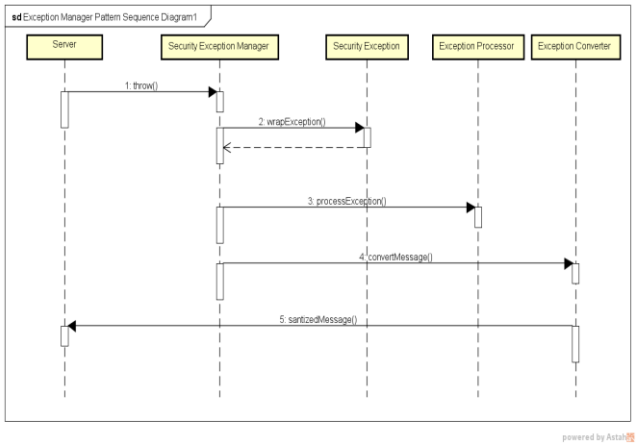

圖 11、Exception Manager Pattern 之循序圖[7]

圖 11 說明 Server 與雲端服務之間溝通的一個過程。假設在連線的時候發生了錯誤，如：雲端服務停止服務、對外連線發生錯誤等。在這部分的話 Server 會將錯誤傳給 Security Exception Manager 進行錯誤處理，處理完後在回傳結果給 Server。

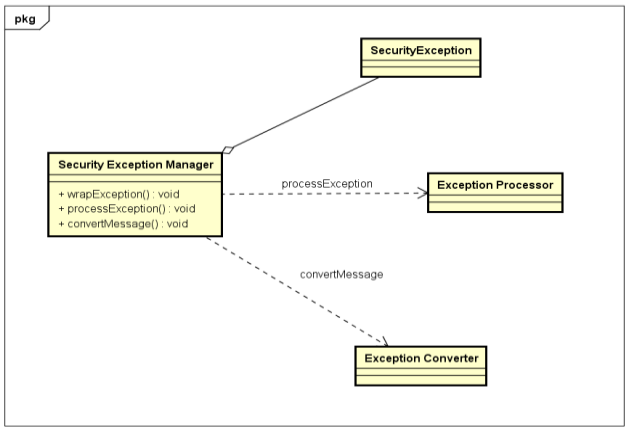

圖 12、Exception Manager Pattern 類別圖[7]

假設系統發生了 Security 的問題 Security Exception Manager 就會接收到該問題資訊並開始進行想過的處理。Exception Processor 就是專門在處理 Exception 的。處理 Exception 之餘，Security Exception Manager 會將相關資訊轉換成信息提供給 Exception Converter 來做記錄。

V. Input Validation Pattern ：

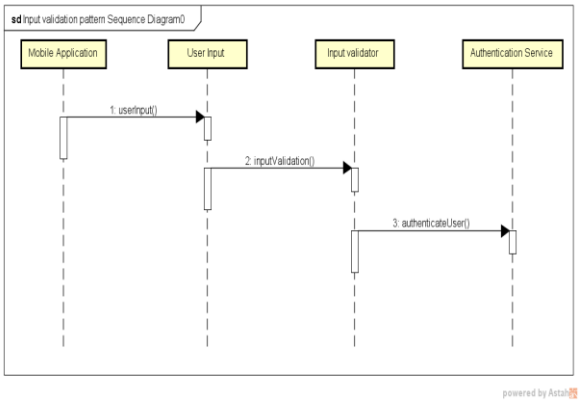

圖 12、Input Validation Pattern 之循序圖

此設計樣式是針對使用者手機端發送輸入信息到 Server 上的部分。圖 12 中 Mobile Application 會先發送使用者所輸入的資料給 Server。Server 會收到後會開始驗證使用者的輸入內容 (User Input)。User Input 的部分是驗證該輸入是否屬於本系統使用者的輸入。若是，則在將資料送給 Input Validator 驗證內容是否安全，最後再一次確認該使用者是否正確。

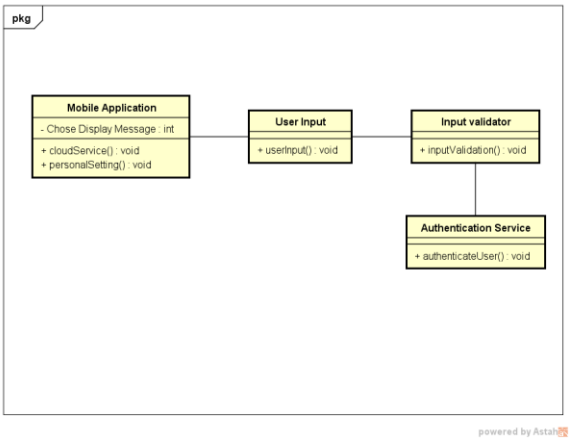

圖 13、Input Validation Pattern 類別圖

當使用者透過手機發出了輸入資訊到 Server 上時，Server 就會透過此設計樣式來檢查使用者的輸入來確認使用者的輸入不包含了敏感字元或惡意程式碼。

六、相關文獻

針對物聯網的相關研究，Kolias 等學者[3]在其研究中以 3 個物聯網主要的安全性問題：

1. 洩漏個人身份信息
   提出了個人化燈控系統，並提出了 3 個問題：
   1.1 未加密的無線通訊。
   1.2 自定義認證方法。
   1.3 廣播使用者辨識信息。
2. 洩漏用戶的敏感信息
   提出遠端遙控澆花系統，並提出以下安全性問題：
   2.1 不安全的 Web 應用程式。
   2.2 未加密的無線通訊。
3. 非授權的執行功能
   提出了自動化控制裝置系統，並提出以下問題：
   3.1 未加密的無線通訊。
   3.2 雲端服務。
   3.3 不安全的網路服務。

在這三個問題中，分別提出了三個實際案例，而 3 個案例都會在裝置間溝通時產生安全問題並針對該案例所產生的安全問題作說明。

Lee 等學者[6]討論所有與物聯網相關之主題。它將物聯網切割成三大類分別是 AI/Autonomics、Wireless Sensor & Actuator Networks 及 Smart Objects。另外也定義了物聯網互動的方式：Human-to-Object Communication & Object-to-Object Communication。此論文提出了物聯網運作流程的架構，並說明了物聯網的運作需求。

七、結論

現今物聯網裝置越來越多，相對的安全性的問題會開始浮現出來。當問題數量到達一定數量後，也許會成為一個很大的科技危機。儘管現在還沒有多少人重視這一個問題。因此，本研究提出了幾個物聯網常見的問題，如：當裝置透過 Wi-Fi 連線時，我們並沒有針對傳輸的資料做加密，有心人士可以透過攔截器來竊取我們傳輸的資料並加以修改。針對這樣的物聯網之安全性問題，本論文提出了使用系統架構圖裝置間之通訊技術探討物聯網的安全議題，並且針對物聯網的安全議題，提出套用五個安全性設計樣式來增加物聯網裝置間的通訊安全性。

本論文提出安全性系統分析與設計流程，針對安全性的方向出發，並輔以軟體工程開發方法，希望在這個資料容易受到威脅的時代，利用軟體工程的方法，一步步抽絲剝繭，分析與設計安全性系統。本研究採用使用案例分析系統需求，並分析使用案例圖及系統活動圖。進一步根據使用案例圖、情節及活動圖建立系統的初始架構。在系統架構中加上安全性樣式設計，完成系統元件與類別的細部設計。

* 本研究接受科技部編號：MOST 104-2221-E-017 -014 -研究計畫經費補助

參考文獻

1. 維基百科, 物聯網 (The Internet of Things); http://wiki.mbalib.com/zh-tw/%E7%89%A9%E8%81%94%E7%BD%91

2. J.Rivera, “Gartner Says 4.9 Billion Connected ‘Things’ Will Be in Use in 2015”, Gartner, 11 Nov. 2014;www.gartner.com/newsroom/id/2905717.
3. Constantion Kolias, Angelos Stavrou, Jeffrey Voas, Irena Bojanova, and Richard Kuhn, “Learning Internet-of-Things Security ‘Hand-On’ ”, IEEE Computer and Reliability Societies, January/February 2016; http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=7397713
4. 維基百科, Arduino; https://zh.wikipedia.org/wiki/Arduino
5. WIKIPEDIA, Security Patterns; https://en.wikipedia.org/wiki/Security_Patterns
6. Gyu Myoung Lee, Noel Crespi, Jun Kyun Choi, Matthieu Boussard, “Internet of Things”, Telecommunication Services Evolution, LNCS 7768, pp. 257–282, 2013; http://link.springer.com/chapter/10.1007/978-3-642-41569-2_13
7. Security Design Patterns; https://sites.google.com/site/designpatternswiki/SecurityDesignPatterns/secure-logger-pattern
8. RFID; http://blog.davidou.org/archives/684
9. RFID; http://here-apps.blogspot.tw/2014/07/lab6-arduino-rfid-checking-system.html
10. 維基百科, 藍牙; https://zh.wikipedia.org/wiki/%E8%97%8D%E7%89%99
11. Microsoft, 藍牙; https://msdn.microsoft.com/en-us/library/windows/desktop/aa362927(v=vs.85).aspx
12. Nobukazu Yoshioka, Hironori Washizaki, and Katsuhisa Maruyama, “A Survey on Security patterns”, Progress in Informatics, No. 5, pp.35–47, (2008); https://www.nii.ac.jp/pi/n5/5_35.pdf
13. Brianne Magouirk Bettcher, Tania Giovannetti, Laura Macmullen, and David J.Libon, “Error detection and correction patterns in dementia: A breakdown of error monitoring processes and their neuropsychological correlates”, Journal of the International Neuropsychological Society (2008), 14, 199–208; http://journals.cambridge.org/download.php?file=%2FINS%2FINS14_02%2FS1355617708080193a.pdf&code=0bc38500a6521ec2b810d4d41529542f