科技部資訊安全技術研發專案計畫

『系統測試計畫書』

System Testing Plan

IoT 可信賴架構之設計與實作

IoT Trusted Architecture

MOST 105-2221-E-011-070-MY3

研究團隊

主持人：吳宗成教授(臺灣科技大學資管系)

共同主持人：羅乃維教授(臺灣科技大學資管系)

查士朝副教授(臺灣科技大學資管系)

葉國暉副教授(東華大學資管系)

左瑞麟副教授(政治大學資學系)

專任研究助理：藍袖瑛(臺灣科技大學資管系)

Department of Information Management,

National Taiwan University of Science and Technology, Taiwan

2017/6/14

目錄

版次變更記錄

版次	變更項目	變更日期
1.0	第一版	2017.06.14

1. 緒論 (Introduction)

本平台 IoT 可信賴架構主要以一般家庭環境為考量，此環境內可分為三類角色：家庭成員(Home Owner)、訪問者(Roaming Visitors)、家庭內受照顧者(Caregivee)等角色，以建置家庭雲端環境相關之安全應用，支援不同的資訊安全應用與服務。本平台所需建置之家庭雲端伺服器包含者身分鑑別與存取控管、藍牙協定安全度檢測機制、行動漫遊裝置之隱私保護、裝置對裝置(M2M)相互鑑別與安全通訊、使用者遠端身分鑑別與服務授權等功能。

第一年(105 年至 106 年)已完成進度是在 IoT 可信賴架構之設計與實作上，呈現以下功能：(1)若使用者向伺服器提出資訊存取需求，需經由身分鑑別模組鑑別該使用者身分是否為合法授權；通過身分鑑別後，依據身分授權，提供不同資料存取權限。(2)檢測行動穿戴裝置與智慧型手機之間的藍牙通訊行為是否安全。(3)在取得 IoT 裝置的服務前，使用者可先得知裝置將蒐集的資訊及其應用目的，並決定是否要使用此裝置所提供的服務。(4)鑑別感測裝置時，需向閘道器進行註冊，並儲存感測裝置識別碼等資訊，以預設連線配對；並在感測裝置之間，進行輕量化的鑑別機制。(5)驗證使用者是否有權存取雲端伺服器資料，並確保資料於閘道器與雲端伺服器之間訊息的機密性及完整性。

本計畫所建構的 IoT 可信賴架構平台，使用者以行動穿戴式裝置與智慧型手機透過閘道器讀取即時或短期個人生理或家庭環境感測之歷史資料，此外，使用者可透過網際網路存取雲端平台上的長期個人生理或家庭環境感測之歷史資料。所有個人生理或家庭環境感測資料皆由佈建於家庭環境的感測器及安裝於受照顧者身上之感測器所提供。本平台之貢獻是提供物聯網環境下的安全資料存取及各角色間身分鑑別功能。

依據本 IoT 可信賴架構平台下列各項子系統將進行各子系統測試以及模組整合測試和接受測試(Acceptance Testing)：

(1) 使用者身分鑑別與存取控管模組

(2) 藍牙協定安全度檢測模組

(3) 行動漫遊裝置之隱私保護模組

(4) 裝置對裝置(M2M)相互鑑別與安全通訊模組

(5) 使用者身分鑑別與安全通訊模組

1.1 測試範圍 (Scope of Testing)

本 IoT 可信賴架構平台的測試計畫，確認在系統整合前，所有的子系統均可正確輸出並順利整合。因此，將著重於整合測試(Integration Test)與接受度測試(Acceptance Test)，進一步找出本系統中的缺失，測試各個子系統於整合時衝突的情況是否會發生。本計畫未使用相關開放原始碼，無與商業軟體比較。進行整合測試的相關計畫與內容，並希望透過此文件的規劃與實踐，達到順利測試並正確執行各子系統，以正確完成本模組之系統整合。

1.2 接受準則 (Acceptance Criteria)

本測試計畫需要滿足下列的測試接受準則：

(1) 行動裝置之 Wi-Fi 通訊功能需正常執行。

(2) 資料存取模組可控管所有使用者存取資料之權限。

(3) 閘道器(Gateway)應用身分鑑別模組鑑別使用者的合法性。

(4) 資料傳輸模組要確保資料可於行動裝置與閘道器間正常傳送與接收。

(5) 使用者介面模組可提供使用者讀取資料。

(6) 取得與接收智慧型行動裝置與智慧型穿戴式裝置間的傳輸封包。

(7) 取得與接收智慧型行動裝置與智慧型穿戴式裝置間的建立連線流程傳輸安全度檢測。

(8) 行動裝置的 BLE 通訊功能需正常執行。

(9) 感測裝置的 BLE 通訊功能需正常執行。

(10) 隱私政策查詢模組需事先載入隱私政策。

(11) 行動裝置的 Android 版本需在 5.0 以上(支援較新的 BLE 模組)。

(12) 閘道器能正確鑑別感測裝置。

(13) 感測裝置能正確鑑別閘道器。

(14) 閘道器與感測裝置能正常傳遞與接收資料。

(15) 連線配對模組與身分鑑別模組以及資料傳輸模組三者能彼此溝通。

(16) 行動裝置之 3G/4G 通訊功能需正常執行。

(17) 多款行動裝置能夠正常於本平台執行。

(18) 使用者能透過身分鑑別模組正確鑑別身份。

(19) 身分鑑別模組能與資料傳輸模組以及加解密模組溝通。

(20) 在 Roaming Access 的部份能夠透過資料傳輸模組安全傳輸。

(21) 各項參數及數據在資料流中能正確的傳遞。

(22) 系統模型可依實際環境變更進行調整。

(23) 測試程序需要依循本測試計畫所訂定的程序進行，且測試結果必須符合預期測試結果方能接受。

(24) 本系統需要對所有列為必要(Critical、Important、Desirable)之需求進行完整測試。

(25) 測試程序需要依照本測試計畫所訂定的程序進行，所有測試結果需要能符合系統需求規格書預期測試結果方能接受。

(26) 以測試案例為單位，當測試未通過時，需要進行該單元的測試，其接受的準則與前一項之規定相同。

2. 測試環境 (Testing Environment)

圖 1 為 IoT 可信賴架構平台進行測試的環境描述：

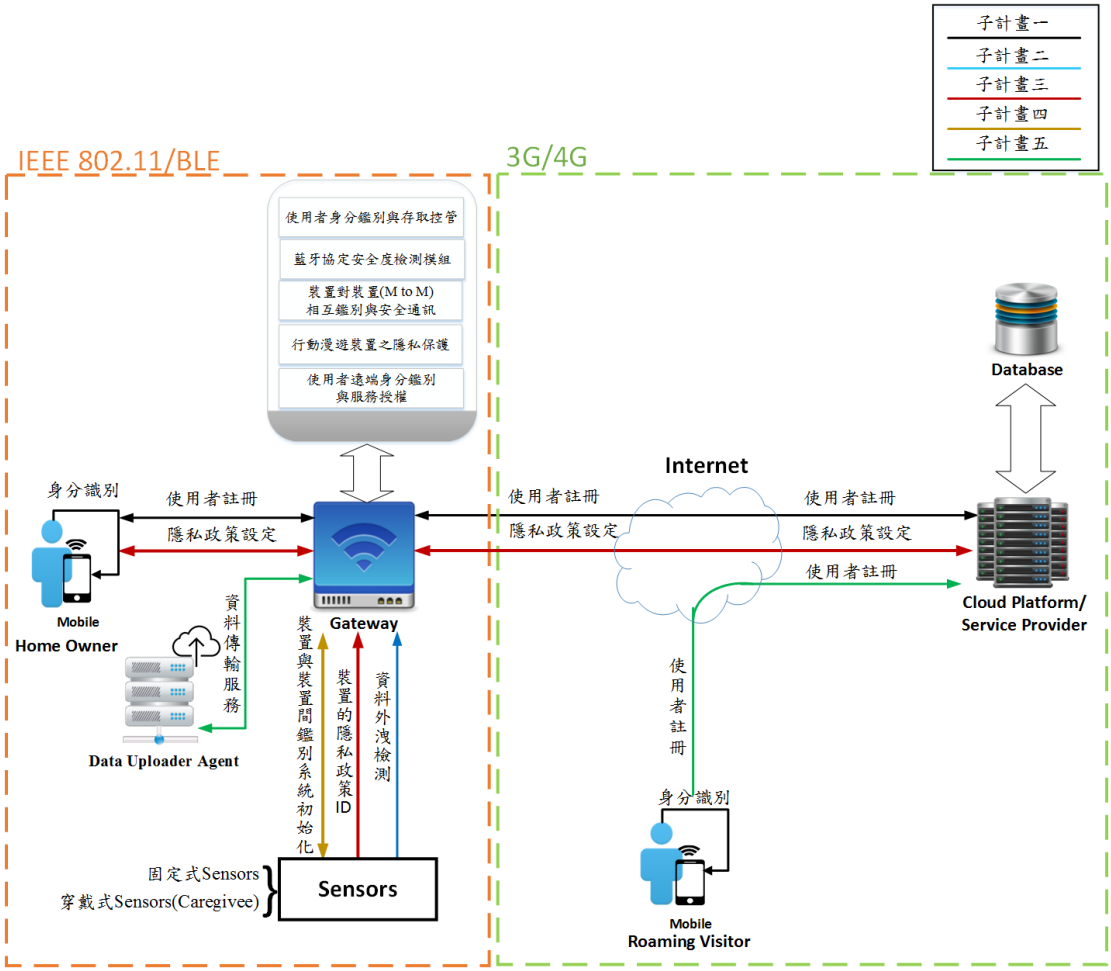


圖1.IoT 可信賴架構之設計與實作-系統設置初始化架構圖

2.1 硬體規格 (Hardware Specification)

依據圖 1 測試環境架構圖內容，進行測試之硬體規格說明，如下列所示：

(1) 使用者端(Home Owner/Roaming Visitor/Service User)：含使用者身分鑑別與存取控管模組、使用者裝置隱私協商模組與使用者介面模組

- Mobile：ZenFone 3
- CPU：Snapdragon™ 625 @2.0Ghz
- RAM：3GB LPDDR3
- ROM：32GB

(2) 閘道器端(Gateway)：含資料傳輸模組、資料存取模組、身分鑑別模組

- 開發板：Raspberry Pi 3 Model B

- 處理器：Broadcom BCM2837 1.2GHz Cortex-A53 1.2GHz 4 核心
- 記憶體：1GB
- 儲存裝置：Kingston microSDXC 16GB U3
- 無線網路：Broadcom BCM43438 2.4GHz 802.11n Wireless
- 藍牙：Broadcom BCM43438 Bluetooth LE 4.1

(3) 感測器(Sensor)裝置：含裝置隱私協商模組、裝置對裝置(M2M)相互鑑別與安全通訊模組、藍牙協定安全度檢測模組

- Arduino Uno
  - 處理器：Atmel ATmega328p
  - SRAM：2Kbytes
  - Flash：32Kbytes
- 藍牙模組：HM-10CC2541 SensorTag：溫濕度感測
- Scosche Rhythm+手臂式心跳帶：綠/黃光學傳感器、心跳感測

(4) 雲端平台(Cloud Platform)伺服器：含隱私政策查詢模組、遠端身分鑑別模組

- CPU：Intel Core i7-3770 3.40 GHz
- RAM：4 GB
- 硬碟空間：500GB

2.2 軟體規格 (Software Specification)

依據圖 1 測試環境架構圖內容，測試環境之軟體規格說明，如下列所示：

(1) 閘道器端(Gateway)

- 開發板：Raspberry Pi 3 Model B
- 作業系統：Android 7.1.2
- 資料庫版本：MYSQL 5.6.19
- 應用程式開發語言：Java

(2) 雲端平台(Cloud Platform)伺服器

- 作業系統：Windows 10 64bits
- 網頁伺服器：Java Servlet/ JSP、Apache Tomcat 7.0.78
- 應用程式開發語言：Java 1.8.0_131
- 資料庫版本：MYSQL 5.7.18

- 應用程式開發語言：Java

(3) 感測器(Sensor)裝置

- 開發板：Arduino Uno
- 開發版系統版本：S132 3.1.0
- 應用程式開發語言：C

(4) 智慧型裝置手機

- 手機作業系統：Android 7.0
- 應用程式開發語言：Java

2.3 測試資料來源 (Test Data Sources)

測試項目	數量	測試來源
註冊功能	一組	最高權限使用者創建一般使用者帳戶
登入功能	一組	可登入並鑑別已創建之帳戶
讀取資料功能	一組	可向閘道器取得相關資訊
權限控管功能	一組	可控管使用者之讀取資訊權限
感測器隱私政策	一組	感測器所預先寫入的範例隱私政策
註冊後的帳號密碼	十組	自行設定之帳號
錯誤的帳號密碼	十組	自行設定之帳號

3. 測試時程、程序與責任(Testing Schedule, Procedure, Responsibility)

3.1 測試時程 (Testing Schedule)

(1) 時程

測試項目	時間
各子系統之內部元件整合測試 (Module Test)	2017/03/19~2017/05/31
ITA 系統整合測試 (Integration Test)	2017/06/01~2017/06/22
ITA 系統接受度測試 (Acceptance Test)	2017/06/23~2017/07/28

(2) 查核

測試項目	時間
各子系統之內部元件整合測試 (Module Test)	2017/06/01
ITA 系統整合測試 (Integration Test)	2017/06/23
ITA 系統接受度測試 (Acceptance Test)	2017/07/29

3.2 測試程序 (Testing Procedure)

各子系統的元件測試，由各子系統的開發負責人執行。待各子系統整合完成後，由全體人員協同執行整體計畫的整合測試。

3.2.1 整合測試(Integration Testing)

IoT 可信賴架構之設計與實作之使用案例(Use Case)，以測試使用者身分鑑別與存取控管模組、藍牙協定安全度檢測模組、行動漫遊裝置之隱私保護模組、裝置對裝置(M2M)相互鑑別與安全通訊模組、使用者身分鑑別與安全通訊模組之整合為目的。

- 模組一(使用者身分鑑別與存取控管模組)如下圖所示：

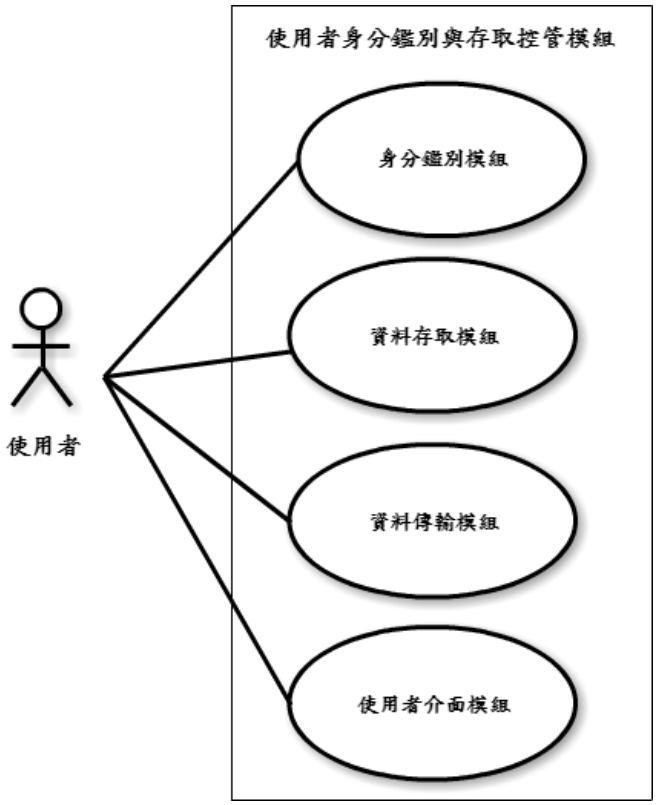


圖2.使用者身分鑑別與存取控管模組之使用案例

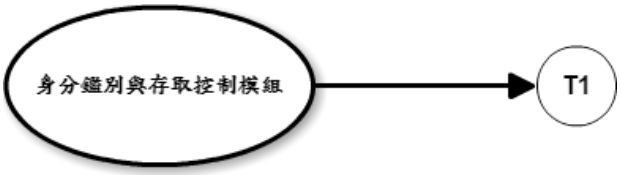


圖3.使用者身分鑑別與存取控管模組接受度測試

✓ 模組二(藍牙協定安全度檢測模組)如下圖所示：

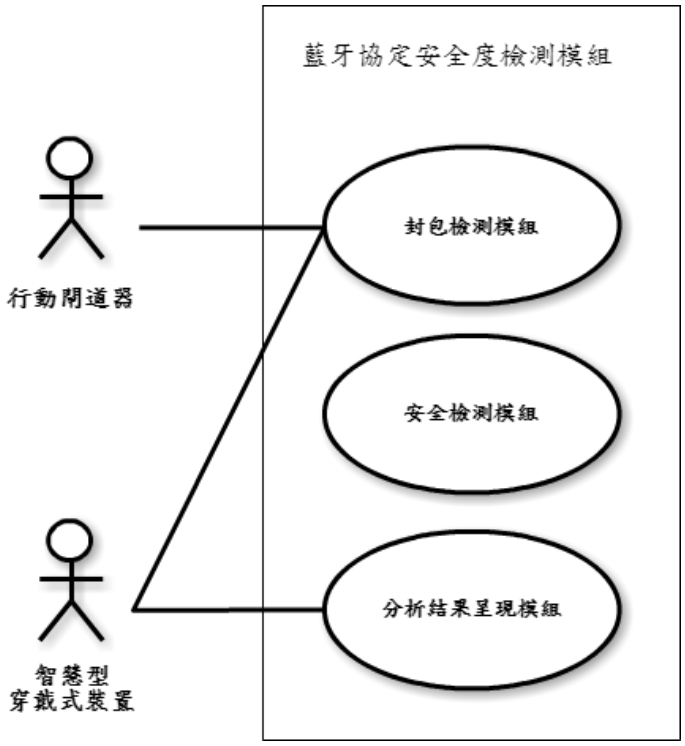


圖4.藍牙協定安全度檢測模組之使用案例

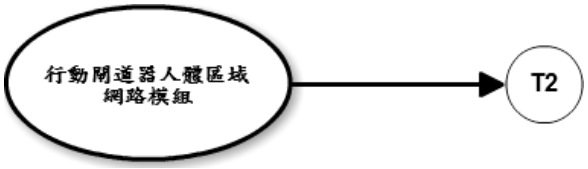


圖5.藍牙協定安全度檢測模組接受度測試

✓ 模組三(行動漫遊裝置之隱私保護模組)如下圖所示：

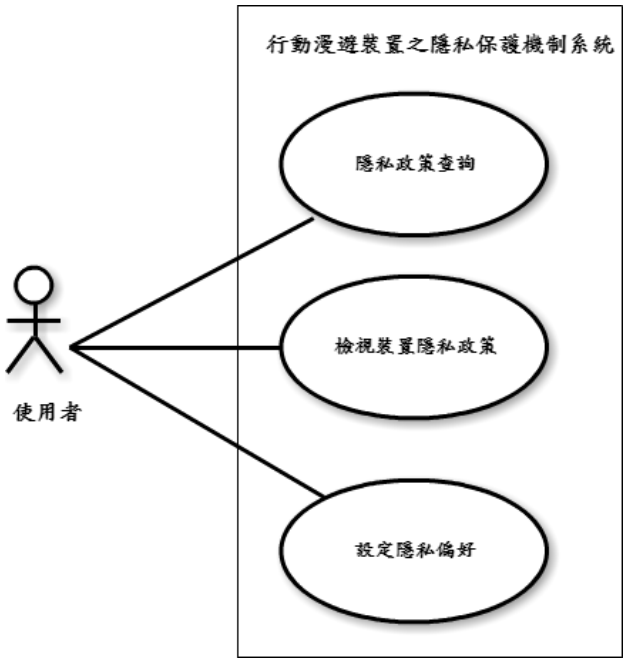


圖6.行動漫遊裝置之隱私保護模組之使用案例

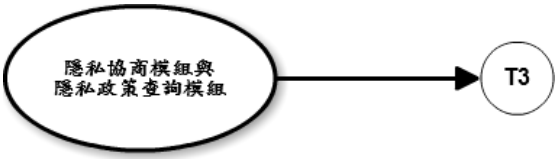


圖7.行動漫遊裝置之隱私保護模組測試

✓ 模組四(裝置對裝置(M2M)相互鑑別與安全通訊模組)如下圖所示：

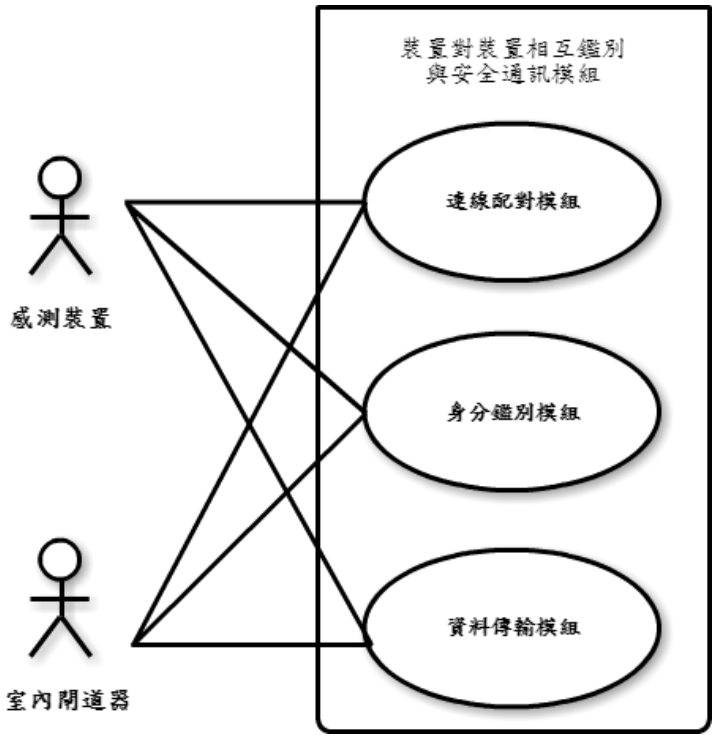


圖8. 裝置對裝置(M2M)相互鑑別與安全通訊模組之使用案例

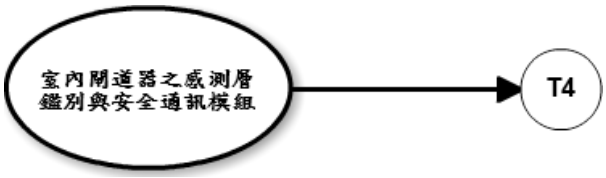


圖9. 裝置對裝置(M2M)相互鑑別與安全通訊模組之接受度測試

✓ 模組五(使用者身分鑑別與安全通訊模組)如下圖所示：

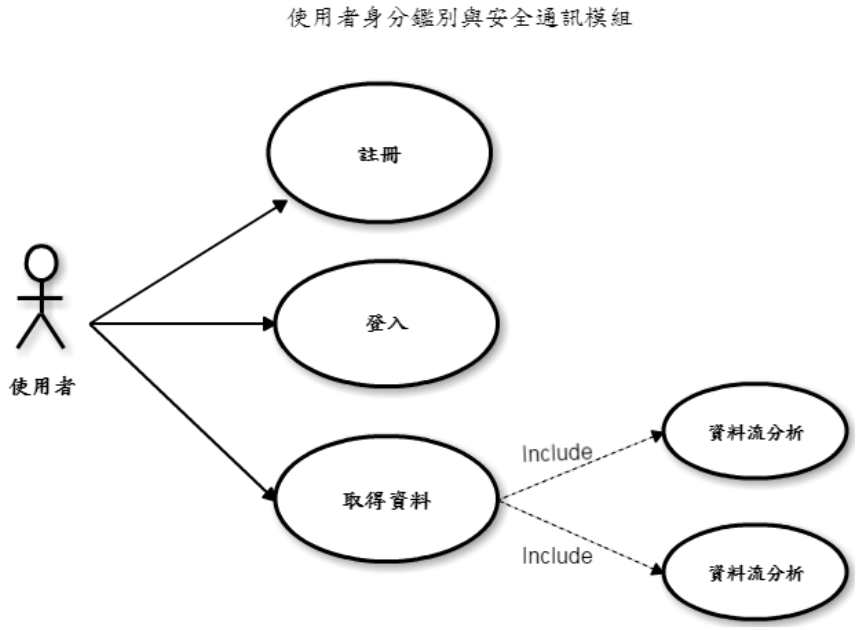


圖10. 使用者身分鑑別與安全通訊模之使用案例

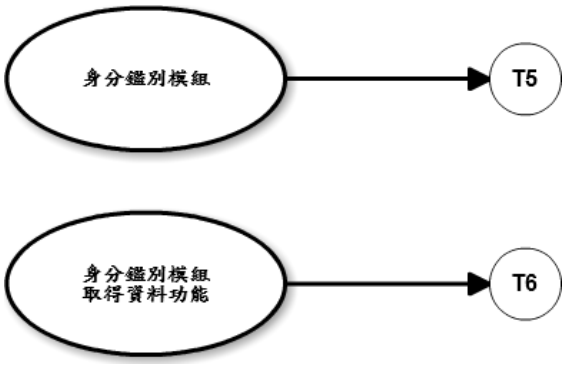


圖11. 使用者身分鑑別與安全通訊模之接受度測試

3.3 人員職責分配 (Personnel Responsibility Assignment)

表1. 人員職責分配表

Testing Activities	Personnel
Acceptance Testing (AT1)	藍袖瑛 吳書樂
Acceptance Testing (AT2)	藍袖瑛 謝欣余
Acceptance Testing (AT3)	藍袖瑛 吳書樂 黃婷瑋
Integration Testing (IT1)	李濬志 蕭詔安 高慧媛 李雅雯
Integration Testing (IT2)	郭峻鴻 李宇正
Integration Testing (IT3)	陳俊甫 蔡宗穎 黃子嘉 彭偉慶
Integration Testing (IT4)	莊祐軒 許勝翔 賴伯融 張守群 黎哲宇
Integration Testing (IT5)	詹琨泰 蕭人和
Integration Testing (IT6)	劉子源 蘇勤文 莊禾暘

3.3.1 接受測試 (Acceptance Testing)

本計畫將進行使用者相關資訊進行系統測試，系統測試流程如下：

使用者(Home Owner/Roaming Visitor/Service User)：使用者對裝置(H2M)負責使用者與行動裝置相互識別。使用者註冊時，需向行動裝置輸入身分識別的機敏資料，確認其存取權限。當遠端使用者欲取得資料時，須先進行身分驗證，驗證通過後，閘道器傳送票據給遠端使用者及雲端資料庫，以便遠端使用者及伺服器溝通取得資料，其中遠端使用者、閘道器以及雲端資料庫三者之間的傳輸資料皆透過加解密傳輸模組進行加密以防止敏感資料遭到竊取。透過智慧型手機運行封包檢測模組擷取穿戴式裝置傳輸的封包，經過安全檢測模組分析確認穿戴式裝置與智慧型手機建立安全連線，再提醒使用者所持有的手機以及穿戴裝置所處的連線模式是否安全。在使用者裝置隱私協商模組會先取得裝置 ID 並連線到伺服器取得完整的隱私政策。接著，透過使用者介面模組將隱私政策呈現給使用者讓使用者決定是否接受該裝置的隱私政策。使用者完成確認後，使用者裝置隱私協商模組將使用者的決定作為使用者的隱私偏好寫入裝置，並在使用者裝置上呈現裝置隱私政策與隱私協商結果。

感測裝置(Sensor)：感測裝置在第一次進行連線配對時向閘道器進行註冊，由閘道器儲存感測裝置識別碼、產生秘密金鑰(Secret Key)等資訊，建立連線配對。確保傳輸資料可於感測裝置與閘道器間正常地傳送與接收。

閘道器(Gateway)：裝置對裝置(M2M)負責行動裝置對閘道的鑑別，使用者註冊後，為確保裝置雙方的合法性，行動裝置需向閘道進行鑑別，進行資料存取。確保資料可於行動裝置與閘道器間正常傳送與接收。藍牙封包側錄將針對感測裝置傳與閘道器中間的傳輸進行封包擷取監聽，並將監聽封包紀錄傳送至安全檢測模組進行傳輸的安全分析。感測裝置傳與閘道器經評估雙方各自的 I/O 能力、運算能力而選定中間，再由閘道器產生秘密金鑰且安全地將秘密金鑰回傳至感測裝置。

雲端平台(Cloud Platform)：當遠端使用者欲取得資料時，須先進行身分驗證，驗證通過後，閘道器傳送票據給遠端使用者及雲端資料庫，以便遠端使用者及伺服器溝通取得資料，其中遠端使用者、閘道器以及雲端資料庫三者之間的傳輸資料皆透過加解密傳輸模組進行加密以防止敏感資料遭到竊取。

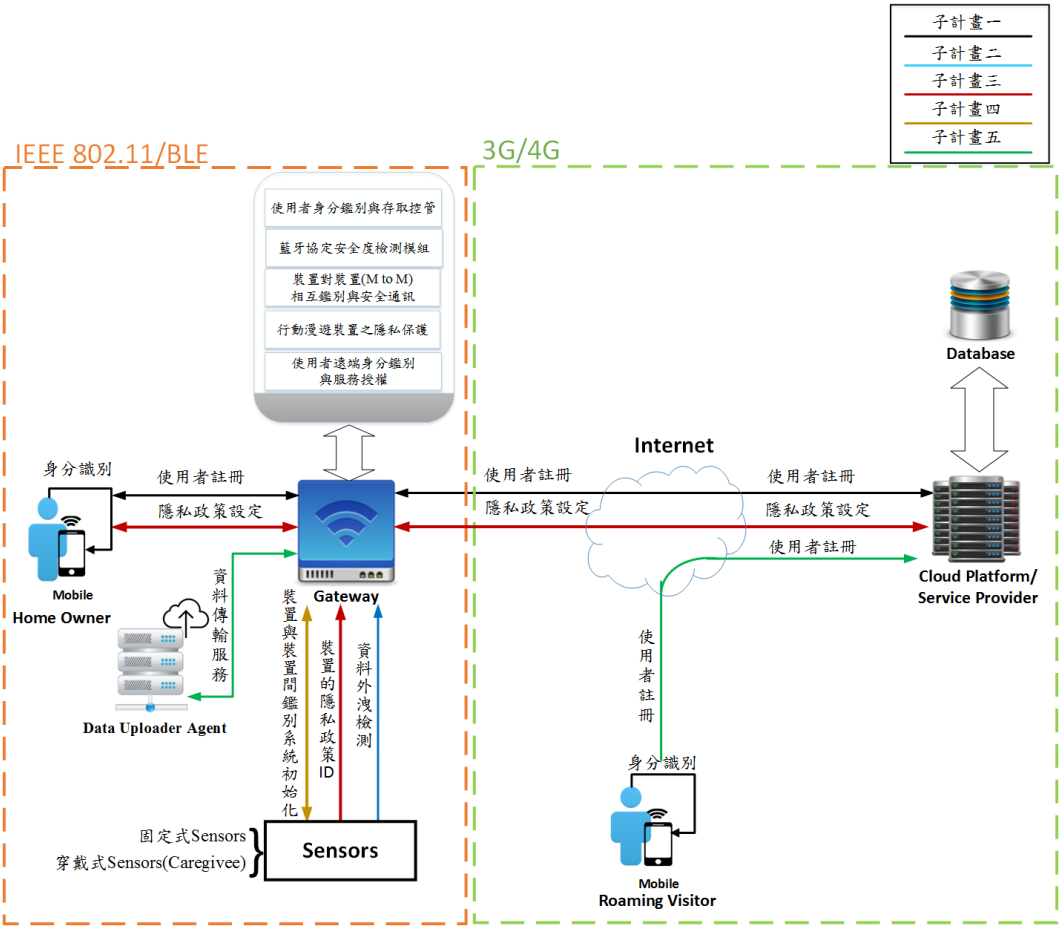


圖12.　IoT 可信賴架構之設計與實作系統流程

再者，將進行系統接受測試，其次序為：AT1→AT2→AT3，AT1 驗證各子系統使用者身分鑑別與存取控管及使用者身分鑑別與安全通訊可正確輸出並順利整合運作，AT2 分析各系統的藍牙協定與隱私保護及裝置對裝置相互鑑別明確列出相關安全與分析，AT3 各子系統需正確執行並符合系統需求規格書[1]之預期測試結果。

ITA：IoT 可信賴架構之設計與實作

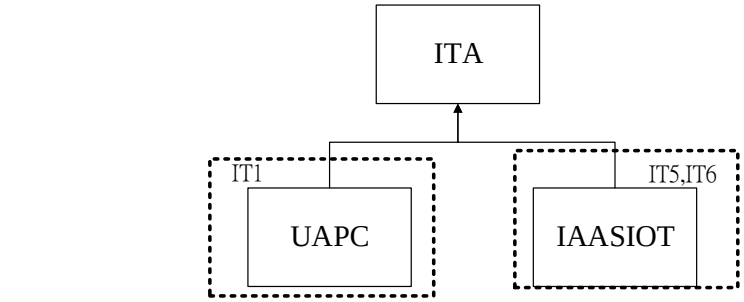
UAPC：使用者身分鑑別與存取控管

SBAN：藍牙協定安全度檢測

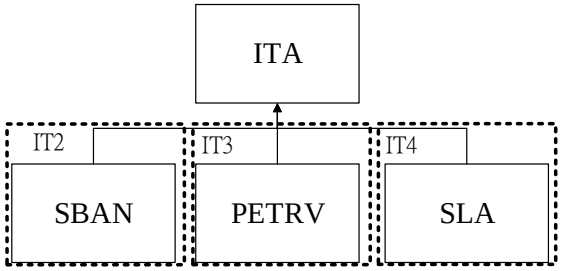
PETRV：行動漫遊裝置之隱私保護

SLA：裝置對裝置(M2M)相互鑑別與安全通訊

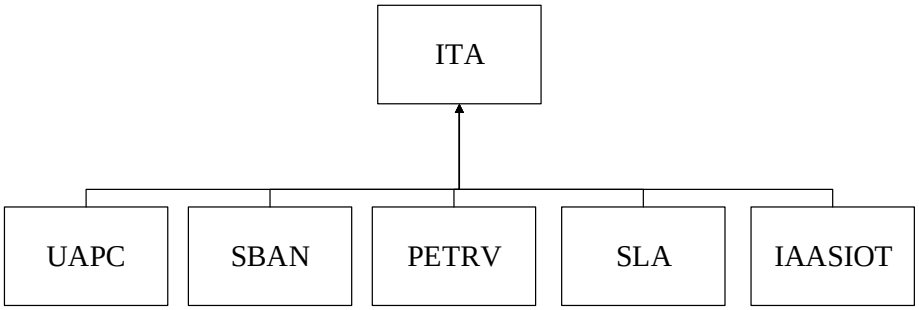
IAASTIOT：使用者身分鑑別與安全通訊



(a)接受度測試 AT1



(b)接受度測試 AT2



(c)接受度測試 AT3

圖13.　IoT 可信賴架構之設計與實作系統整合與可接受度測試架構圖

4. 測試案例 (Test Cases)

4.1 整合測試案例 (Integration Testing Cases)

4.1.1 IT1 測試案例

目的：

(1) 驗證使用案例 1。

(2) 室內使用者透過 Wi-Fi 連接閘道進行使用者之身分鑑別。

(3) 使用者能依據自身權限存取資料並瀏覽即時資料。

表2. IT1 測試案例

Identification	IT1	
Name	使用者鑑別協定與控管機制系統之整合測試	
Tested target	使用者鑑別協定與控管機制系統	
Reference	UAPC-DIC-001、UAPC-UIR-001、UAPC-EIR-001、UAPC-EIR-002、UAPC-ENR-001、UAPC-MTR-001	
Severity	Level 1 (Critical)	
Instructions	*Actor actions*	*System responses*
	1.使用者點開 App	
		2.帳號、密碼輸入畫面
	3.輸入帳號、密碼	
		4.Gateway 驗證資料是否正確
	5.App 使用者登入成功	
	6.進入瀏覽即時資料畫面	
		7.Gateway 傳輸 Sensor 之即時資料
	8.瀏覽 Sensor 之即時資料	
Expected result	1.可正確鑑別 App 使用者身分 2.順利存取資料並瀏覽即時資料	
Cleanup	無	

4.1.2 IT2 測試案例

目的：

(1) 驗證使用案例 2。

(2) 驗證封包檢測模組是否能測錄智穿戴裝置與智慧型行動裝置傳輸。

(3) 驗證安全檢測模組是否能分析測錄封包。

表3. IT2 測試案例

Identification	IT2	
Name	行動閘道器上之安全人體區域網路之整合測試	
Tested target	SBAN	
Reference	SBAN-FNR-001、SBAN-FNR-002	
Severity	Level 1 (Critical)	
Instructions	*Actor actions*	*System responses*
	1.穿戴裝置與行動裝置進行連線配對	
		2.封包檢測模組對穿戴裝置與行動裝置間傳輸進行測錄
	3.穿戴裝置與行動裝置在連線配對完成後，測錄封包進行分析	
		4.取得安全檢測結果
Expected result	1.進行配對後可以驗證智慧型穿戴裝置與智慧型行動裝置彼此連線封包是否被側錄 2.在安全的狀況下進行資料傳輸	
Cleanup	無	

4.1.3 IT3 測試案例

目的：

(1) 驗證使用案例 3。

(2) 使用者針對裝置設定隱私偏好。

(3) 使用者能檢視與隱私偏好相對應的服務結果。

表4. IT3 測試案例

Identification	IT3	
Name	隱私協商模組與隱私政策查詢模組之整合測試	
Tested target	[PETRV1.0.0]	
Reference	PETRV-FNR-001、PETRV-FNR-002	
Severity	Level 1 (Critical)	
Instructions	*Actor actions*	*System responses*
	1.使用者取得周邊裝置清單，並選擇欲使用的裝置，接著查詢裝置的隱私政策	
		2.伺服器在收到查詢裝置隱私政策的要求之後，存取資料庫查詢相對應的隱私政策
	3.使用者閱讀並根據隱私政策，設定隱私偏好。接著將隱私偏好寫入感測裝置(Sensor)	
		4.裝置根據使用者所選擇隱私偏好提供服務
	5.使用者取得服務結果	
Expected result	1.使用者設定隱私偏好，接著使用服務 2.使用者可以正確檢視服務結果	
Cleanup	無	

4.1.4 IT4 測試案例

目的：

(1) 驗證使用案例 4。

(2) 驗證感測裝置是否能正確鑑別閘道器。

(3) 驗證閘道器是否能正確鑑別感測裝置。

(4) 驗證感測裝置與閘道器之間的資料傳輸是否能正常傳送與接收。

表5. IT4 測試案例

Identification	IT4	
Name	物聯網裝置與閘道器之感測層鑑別與安全通訊技術模組(SLA)之整合測試	
Tested target	SLA	
Reference	SLA-FNR-001、SLA-FNR-002、SLA-FNR-003	
Severity	Level 1 (Critical)	
Instructions	*Actor actions*	*System responses*
	1.感測裝置在第一次進行連線配對時向閘道器進行註冊，由閘道器儲存感測裝置識別碼等資訊，建立連線配對	
		2.閘道器連線配對模組產生配對結果並回傳
	3.感測裝置接收配對結果，若成功配對則進行感測裝置與閘道器相互的安全身分鑑別機制	
		4.感測裝置與閘道器互相驗證彼此的身分合法性，並個別將身分鑑別結果回傳
	5.若驗證感測裝置與閘道器身分皆合法，則將感測裝置所感測的資料以安全的方式傳送給閘道器	
		6.閘道器持續將接收的感測資料存入資料庫中
		7.每過一段特定的時間，閘道器將會把感測資料傳送至雲端伺服器
Expected result	1.進行鑑別後可以正確驗證感測裝置與閘道器彼此的身分合法性、傳輸資料之完整性	

	2.在安全的狀況下進行感測資料傳輸閘道器可接收來自感測裝置所蒐集之感測資料
Cleanup	清除解密過的分離程式檔

4.1.5 IT5 測試案例

目的：

(1) 驗證使用案例 5。

(2) 使用者透過身分驗證模組將帳號密碼傳至伺服器，檢測伺服器需正確收到資料，並驗證使用者身分是否正確。

(3) 伺服器若驗證使用者身分正確，則回傳 token。

表6. IT5 測試案例

Identification	IT5	
Name	身分鑑別模組登入功能	
Tested target	[IaaSIoT 1.0.0]	
Reference	IAASIoT-FNR-001、IAASIoT-FNR-002、IAAIoT-FNR-003	
Severity	Level 1 (Critical)	
Instructions	*Actor actions*	*System responses*
	1.使用者輸入帳號密碼進行登入	
		2.系統收到資料後，進行身分比對，回傳 token
	3.利用此 token 取得資料	
Expected result	使用者可進入取得資料頁面	
Cleanup	無	

4.1.6 IT6 測試案例

目的：

(4) 驗證使用案例 6。

(5) 使用者傳送取得資料的需求(包含 ID 及加密後的 token)至伺服器，伺服器需正確收到資料，並驗證所傳來資料中的 token 是否正確。

(6) 伺服器驗證正確則回傳資料。

表7. IT6 測試案例

Identification	IT6	
Name	身分鑑別模組取得資料功能	
Tested target	[IAASIoT 1.0.0]	
Reference	IAASIoT-FNR-001、IAASIoT-FNR-002 IAASIoT-FNR-003	
Severity	Level 1 (Critical)	
Instructions	*Actor actions*	*System responses*
	1.使用者按下取得即時資料按鈕，傳送取得資料的需求至 Gateway	
		2.Gateway 驗證 token 是否正確，並回傳結果
	3.使用者按下取得歷史資料按鈕，傳送取得資料的需求至 Server	
		4.Server 驗證 token 是否正確，並回傳結果
	3.利用此 Token 取得資料	
Expected result	使用者可進入取得資料頁面	
Cleanup	無	

4.2 接受測試案例 (Acceptance Testing Cases)

4.2.1 AT1 測試案例

目的：

(1) 驗證 UAPC、IAASIOT 能依流程正確整合運作。

(2) 室內使用者透過 Wi-Fi 連接閘道進行使用者之身分鑑別。

(3) 使用者能依據自身權限存取資料並瀏覽即時資料。

(4) 使用者透過身分驗證模組將帳號密碼傳至伺服器，檢測伺服器需正確收到資料，並驗證使用者身分是否正確。

(5) 伺服器若驗證使用者身分正確，則回傳 token。

表8. AT1 測試案例

Identification	AT1
Name	UAPC、IAASIOT 整合至 ITA
Tested target	UAPC、IAASIOT
Reference	UAPC-DIC-001 、 UAPC-UIR-001 、 UAPC-EIR-001 、 UAPC-EIR-002、UAPC-ENR-001、UAPC-MTR-001 IAASIoT-FNR-001、IAASIoT-FNR-002、IAAIoT-FNR-003
Severity	Level 1 (Critical)
Instructions & Expected result	1. 使用者點開 App 及輸入帳號、密碼 2. 系統收到資料後，進行身分比對，回傳 token 3. 登入成功後，使用者可進入取得資料頁面，選擇讀取即時資料或歷史資料畫面
Cleanup	無

4.2.3 AT2 測試案例

目的：

(1) 驗證 SBAN、PETRV、SLA 能正確執行風險評估功能。

(2) 驗證封包檢測模組是否能測錄智穿戴裝置與智慧型行動裝置傳輸。

(3) 使用者針對裝置設定隱私偏好。

(4) 使用者能檢視與隱私偏好相對應的服務結果。

(5) 驗證感測裝置是否能正確鑑別閘道器。

(6) 驗證閘道器是否能正確鑑別感測裝置。

(7) 驗證感測裝置與閘道器之間的資料傳輸是否能正常傳送與接收。

表9. AT2 測試案例

Identification	AT2
Name	SBAN、PETRV、SLA 整合至 ITA
Tested target	SBAN、PETRV、SLA
Reference	SBAN-FNR-001、SBAN-FNR-002、PETRV-FNR-001、PETRV-FNR-002、SLA-FNR-001、SLA-FNR-002、SLA-FNR-003
Severity	Level 2 (Important)
Instructions & Expected result	1. 穿戴裝置與行動裝置進行第一次連線配對 2. 連線配對完成後，測錄封包進行分析 3. 使用者取得周邊裝置清單，並選擇欲使用的裝置，接著查詢裝置的隱私政策 4. 使用者閱讀並根據隱私政策，設定隱私偏好 5. 將隱私偏好寫入感測裝置(Sensor) 6. 使用者取得服務結果 7. 進行感測裝置與閘道器身分皆合法，鑑別後可以正確驗證感測裝置與閘道器彼此的身分合法性、傳輸資料之完整性
Cleanup	無

4.2.4 AT3 測試案例

目的：

(1) 在 AT1 與 AT2 測試成功的基礎上，再次重覆驗證 UAPC、IAASIOT、SBAN、PETRV、SLA 能正確地整合於 ITA 架構。

(2) 驗證 ITA 所有功能與流程能正確整合運作。

表10. AT3 測試案例

Identification	AT3
Name	UAPC、IAASIOT、SBAN、PETRV、SLA 整合至 ITA
Tested target	UAPC、IAASIOT、SBAN、PETRV、SLA
Reference	UAPC-DIC-001 、 UAPC-UIR-001 、 UAPC-EIR-001 、 UAPC-EIR-002、UAPC-ENR-001、UAPC-MTR-001 IAASIoT-FNR-001、IAASIoT-FNR-002、IAAIoT-FNR-003 SBAN-FNR-001、SBAN-FNR-002、PETRV-FNR-001、 PETRV-FNR-002、SLA-FNR-001、SLA-FNR-002、 SLA-FNR-003
Severity	Level 2 (Important)
Instructions & Expected result	1. 使用者點開 App 及輸入帳號、密碼 2. 系統收到資料後，進行身分比對，回傳 token 3. 登入成功後，使用者可進入取得資料頁面，選擇讀取即時資料或歷史資料畫面 4. 穿戴裝置與行動裝置進行第一次連線配對 5. 連線配對完成後，測錄封包進行分析 6. 使用者取得周邊裝置清單，並選擇欲使用的裝置，接著查詢裝置的隱私政策 7. 使用者閱讀並根據隱私政策，設定隱私偏好 8. 將隱私偏好寫入感測裝置(Sensor) 9. 使用者取得服務結果 10. 進行感測裝置與閘道器身分皆合法，鑑別後可以正確驗證感測裝置與閘道器彼此的身分合法性、傳輸資料之完整性
Cleanup	無

5. 測試結果與分析 (Test Results and Analysis)

5.1 整合測試案例 (Integration Testing Cases)

表11. 整合測試案例結果

Test Case #	Results (Pass/Fail)	Comment
IT1	Pass	測試通過
IT2	Pass	測試通過
IT3	Pass	測試通過
IT4	Pass	測試通過
IT5	Pass	測試通過
IT6	Pass	測試通過

5.2 接受測試案例 (Acceptance Testing Cases)

表12. 接受度測試案例結果

Test Case #	Results (Pass/Fail)	Comment
AT1	Pass	測試通過
AT2	Pass	測試通過
AT3	Pass	測試通過

Appendix A： 追朔表 Traceability

A.1. 子系統 vs. 測試案例 (Subsystems vs. Test Cases)

表13. Subsystems vs. Test Cases Traceability Table

Test Cases / Subsystems	IT1	IT2	IT3	IT4	IT5	IT6
UAPC-DIC-001	✓					
UAPC-UIR-001	✓					
UAPC-EIR-001	✓					
UAPC-EIR-002	✓					
UAPC-ENR-001	✓					
UAPC-MTR-001	✓					
SBAN-FNR-001		✓				
SBAN-FNR-002		✓				
PETRV-FNR-001			✓			
PETRV-FNR-002			✓			
SLA-FNR-001				✓		
SLA-FNR-002				✓		
SLA-FNR-003				✓		
IAASIOT-FNR-001					✓	✓
IAASIOT-FNR-002					✓	✓
IAASIOT-FNR-003					✓	✓

A.2. 需求 vs. 測試案例 (Requirements vs. Test Cases)

表14. Requirements vs. Test Cases Traceability Table

Test Cases / Requirements	UAPC	SBAN	PETRV	SLA	IAASIOT
AT1	✓				✓
AT2		✓	✓	✓	
AT3	✓	✓	✓	✓	✓

Appendix B： 參考資料 (References)

[1] 國立台灣科技大學吳宗成教授研究團隊，IoT 可信賴架構之設計與實作需求規格書，民國一零五年十二月一日。