**科技部資訊安全實務研發計畫**

**『系統測試報告書』**

**System Testing Document**

**Of**

**CyberSecurity Practices and Research(CPR) Project**

**先進駕駛輔助系統之雲端輔助設計優化--階層式智慧物聯雲於先進駕駛輔助系統優化之應用研究**

**(Cloud Aided Design Optimization for Advanced Driver Assistance Systems--Hierarchical Intelligent Clouds of Things for Optimization of Advanced Driver Assistance Systems)**

**MOST 105-2221-E-327-027-**

**研究團隊**

|  |  |  |
| --- | --- | --- |
| **主持人** | **：** | **陳朝烈 副教授**  **(國立高雄第一科大電子工程學系)** |
| **共同主持人** | **：** | **蘇維宗 助理教授**  **(真理大學資訊工程學系)**  **陳朝鈞 副教授**  **(國立成功大學資訊工程系)** |

**Department of Electronic Engineering,**

**National Kaohsiung First University of Science and Technology,**

**Taiwan**

**2018/05/15**

**目錄**

[1 SECTION 1 INTRODUCTION 5](#_Toc390532938)

[1.1測試範圍 (SCOPE OF TESTING) 9](#_Toc390532939)

[1.2接受準則 (ACCEPTANCE CRITERIA) 9](#_Toc390532940)

[2 S ECTION 2 TESTING ENVIRONMENT 10](#_Toc390532941)

[2.1硬體規格 (HARDWARE SPECIFICATION) 10](#_Toc390532942)

[2.2軟體規格 (SOFTWARE SPECIFICATION) 11](#_Toc390532943)

[2.3測試資料來源 (TEST DATA SOURCES) 11](#_Toc390532944)

[3 SECTION 3 TESTING SCHEDULE, PR OCEDURE, AND RESPONSIBILITY 11](#_Toc390532945)

[3.1測試時程 (TESTING SCHEDULE) 11](#_Toc390532946)

[3.2測試程序 (TESTING PROCEDURE) 12](#_Toc390532947)

[3.2.1整合測試 (Integration Testing) 12](#_Toc390532948)

[3.3人員職責分配 (PERSONNEL RESPONSIBILITY ASSIGNMENT) 12](#_Toc390532949)

[3.3.1接受測試 (ACCEPTANCE TESTING) 13](#_Toc390532950)

[4 SECTION 4 TEST CASE 13](#_Toc390532951)

[5 TEST RESULT AND ANALYSIS 16](#_Toc390532952)

[5.1 整合測試案例 (INTEGRATION TESTING CASES) 16](#_Toc390532953)

[5.2 接受測試案例 (ACCEPTANCE TESTING CASES) 16](#_Toc390532954)

[TRACEABILITY 17](#_Toc390532955)

[GLOSSARY 17](#_Toc390532956)

[REFERENCE 17](#_Toc390532957)

[總計畫兼子計畫一測試報告 18](#_Toc390532958)

[1 SECTION 1 INTRODUCTION 18](#_Toc390532959)

[1.1測試範圍 (SCOPE OF TESTING) 19](#_Toc390532960)

[1.2接受準則 (ACCEPTANCE CRITERIA) 19](#_Toc390532961)

[2 SECTION 2 TESTING ENVIRONMENT 20](#_Toc390532962)

[2.1硬體規格 (HARDWARE SPECIFICATION) 21](#_Toc390532963)

[2.2軟體規格 (SOFTWARE SPECIFICATION) 21](#_Toc390532964)

[2.3測試資料來源 (TEST DATA SOURCES) 21](#_Toc390532965)

[3 SECTION 3 TESTING SCHEDULE, PR OCEDURE, AND RESPONSIBILITY 22](#_Toc390532966)

[3.1測試時程 (TESTING SCHEDULE) 22](#_Toc390532967)

[3.2測試程序 (TESTING PROCEDURE) 22](#_Toc390532968)

[3.2.1整合測試 (Integration Testing) 22](#_Toc390532969)

[3.2.2接受測試 (Acceptance Testing) 24](#_Toc390532970)

[3.3人員職責分配 (PERSONNEL RESPONSIBILITY ASSIGNMENT) 25](#_Toc390532971)

[4 SECTION 4 TEST CASE 26](#_Toc390532972)

[4.1 整合測試案例 (INTEGRATION TESTING CASES) 26](#_Toc390532973)

[4.1.1 IT1測試案例 26](#_Toc390532974)

[4.1.2 IT2測試案例 27](#_Toc390532975)

[4.1.3 IT3測試案例 27](#_Toc390532976)

[4.1.4 IT4測試案例 28](#_Toc390532977)

[4.2接受測試案例 (Acceptance Testing Cases) 28](#_Toc390532981)

[4.2.1 AT1 Test Case 28](#_Toc390532982)

[4.2.2 AT2 Test Case 28](#_Toc390532983)

[4.2.3AT3 Test Case 29](#_Toc390532984)

[4.2.4 AT4 Test Case 30](#_Toc390532985)

[5 TEST RESULT AND ANALYSIS 30](#_Toc390532988)

[5.1 整合測試案例 (INTEGRATION TESTING CASES) 30](#_Toc390532989)

[TRACEABILITY 31](#_Toc390532990)

[附錄一 33](#_Toc390532991)

[附錄二 44](#_Toc390532992)

**文件版本修正履歷表**

|  |  |  |  |
| --- | --- | --- | --- |
| **版次** | **變更項目** | **變更日期** | **紀錄** |
| 1.1.0 | 初版 | 2018/04/25 |  |
| 1.1.1 | 校正 | 2018/04/30 |  |
| 1.1.2 | 校正 | 2018/05/05 |  |

# 總計畫兼子計畫一

# 1 SECTION 1 INTRODUCTION

**本計劃系統總體目標：**

本計畫主要以先進駕駛輔助系統(Advanced Driver Assistance System, ADAS)為例，建構一彈性化開發平台，以期未來能開發工業4.0各種應用。ADAS內部最主要的部份為影像處理子系統，也是自駕車內必備的先導技術，例如加入LiDAR (light detection and ranging)之後，可以提供3D的立體視覺給ADAS子系統進行各種路況的精確判斷。然而，影響影像處理效果的因素眾多，因此很難設計一通用於各種狀況與個人習慣之自適性ADAS系統，而ADAS系統影響駕駛之安全性甚鉅，聯合國也逐年建立法規供各國制定時之參考，儼然成為各汽車大廠角逐市場的重要標的，然舉凡各汽車大廠之展示，均限制場域環境，包含電動車大廠Tesla也警告駕駛人，不可完全依賴自動駕駛，主要就是因為影像處理例外狀況很多。因此，ADAS出廠後逐步改善有其必要性，更是利用工業4.0相關技術可以改善的明確標的之一，輔以車輛本身的其它各種感測器、車輛之間的即時互動，自駕車才有可能達到Level 5的等級，也就是完全自動駕駛，對於國內研發Level 1~4階段的廠商更有幫助，有利於國際市場競爭中取得先機。

**系統特色：**

本計畫整合三個子計畫，分別是：

* 總計畫連結智慧城市以及車廠需求，以OBD-II感測, CAN bus等車用電子相關嵌入式技術，將感測資料連結時序性影像資料，建立完整行車紀錄，提供隨時調閱。並建立深度學習框架，以隨時可以取得機器訓練資料樣本、持續演化精進機器學習模型。
* 子計畫一以行動裝置分攤運算、邊緣運算、行動SDN與NFV技術建構階層式智慧物聯雲，以調閱廣大車機中的ADAS例外樣本和更新車機。並將FPGA晶片實現之ADAS相關產學合作之成果加以運用，作為影像處理的範例。
* 子計畫二負責建置分散式雲端資料庫，提供巨量資料存取平台來對車載感測資料、使用者履歷資料等檔案進行存取管理，並提供基於大數據、機器學習等技術之智慧化分析與優化應用的巨量資料運算與處理平台。
* 子計畫三負責研發安全物聯網應用開發方法，主要核心技術包含建立虛擬私有物聯網(virtual private IoT, VP-IoT)提供安全的物聯網資料交換；另外將運用區塊鍊(blockchain)技術中不易竄改的特性實現基於免疫系統之自主安全ADAS應用開發方法。計畫目標包含維持物聯網中資料之完整性、秘密性、與隱私性以及節點異常行為預防與偵測。

**編號說明:**

|  |  |  |
| --- | --- | --- |
| **需求編號** | **優先順序** | **需求描述** |
| R17-NET-01 |  | 使用者可即時在網頁上觀看直播或者預存的車輛資訊。 |
| R17-DB-01 |  | 於伺服器上建立網頁伺服器服務。 |
| R17-DB-02 |  | 接收使用者觀看車輛資訊要求並傳送要求至車輛。 |
| R17-IT-01 |  | 車機接收伺服器要求並回傳車輛資訊。 |
| R18-NET-01 |  | 使用者可於網頁伺服器上觀看直播預錄影像資料。 |
| R18-DB-01 |  | 於網頁伺服器上建立影像串流功能。 |
| R18-DB-02 |  | 接收使用者觀看車輛影像要求並傳送要求至車輛。 |
| R18-IT-01 |  | 車機接收伺服器要求並回傳車輛影像。 |
| R19-NET-01 |  | 開發使用者可透過系統建立MMCN聯網。 |
| R19-DB-01 |  | 透過MMCN聯網將車輛資訊連結至大數據平台。 |
| R20-NET-01 |  | 開發使用者及車機使用者可透過MMCN聯網儲存車輛資訊。 |
| R20-IT-01 |  | 車機可透過MMCN聯網儲存車輛資訊。 |
| R21-NET-01 |  | 車機使用者可於任意時間、地點及網路讀取車輛資訊或更新資料。 |
| R21-DB-01 |  | 伺服器可接收車機使用者之讀取或修改要求。 |
| R21-IT-01 |  | 車機可向伺服器確認要求，並回傳讀取結果或更新車機資料。 |
| R22-NET-01 |  | 開發使用者可在任意平台上，使用瀏覽器觀看車輛影片及感測資料。 |
| R22-DB-01 |  | 伺服器須提供跨平台服務之功能。 |

本系統的接受度測試所列各子系統所有功能如下表所示:

**系統功能規格:**

* 子計畫一(建立行動裝置的邊緣/霧運算(Device-centric edge/fog computing)環境，以即時蒐集資料、儲存和分析)：
* 蒐集：將行車視訊片段加入時間戳記，車輛感測資料格格式化為JASON，視訊片段和車輛感測資料整理成束(bundle)，再行加密並以URL位址建立索引。此部分成果以利用在高速鐵路VoD, CCTV, 以及市政府交通路口CCTV計畫中。
* 儲存: 所有的行車資料均儲存在行動裝置(車機)內，在需要的時候才回存到資料中心(data center)的大數據平台(Hadoop Distributed File System, HDFS)。需要的時機包含：機器學習需要訓練樣本的時候，以及工程人員調閱的時候。
* 分析：沿著路徑分攤運算，並分享運算資源，路徑上的運算裝置包含行動裝置、路邊裝置(Road-Side Unit, RSU)、邊緣網路功能設備(例如Edge Router)、區域伺服器、以及最後台的資料中心。
* 服務：包含車主服務：更新車輛演算法、提供例外案例；車廠人員服務：調閱例外資料，AI與影像演算法參數模擬。

以上若以Fog/Edge運算工作來分可以分成：

* 行動SDN：由行動裝置以及邊緣路由器建立行動式軟體定義網路(Mobile Software-Define Network, Mobile SDN)，控制面(control plane)互通控制訊息以分析較佳樣本束傳遞路徑、設定虛擬網路功能節點(Virtualized Network Node)轉傳樣本束以及擴散機器學習更新模型，以網路虛擬化(Network Function Virtualization, NFV)技術完成資料面(data plane)之構面。
* 視訊處理：視訊轉碼(transcoding)切片(Slicing)、將視訊切片與感測資料暫存在車機、RSU儲存裝置、以及區域伺服器，並完成RSU路邊裝置的車輛辨識與車流分析，提供政府交通管理單位參考以及未來機器學習與車廠工程師調閱。
* 子計畫二：
* 大量資料壓縮技術
* 機器學習智慧型分析技術的運算環境
* 大量使用者履歷資料整理儲存
* 大量存取負載平衡
* 車主服務
* 車廠人員服務
* 子計畫三：
* 提供物聯網端點屬性加密技術(加密、存取控制、隱私保護)
* 虛擬私有物聯網技術(VP-IoT)
* 以區塊鍊技術實現身分驗證
* 資料完整性驗證
* 與物聯網自主安全方法

**系統外部介面規格:**

|  |  |  |
| --- | --- | --- |
| **需求編號** | **優先順序** | **需求描述** |
| EX1 | 1 | 車機道路駕駛影像。 |
| EX2 | 1 | 車機OBDII模擬感測資料。 |
| EX3 | 1 | 路邊裝置影像。 |
| EX4 | 1 | 由使用者設定欲修改之車機或路邊裝置之資料。 |

**系統內部介面規格:**

|  |  |  |
| --- | --- | --- |
| **需求編號** | **優先順序** | **需求描述** |
| IN1 | 1 | 接收車機道路駕駛影像並儲存成影片。 |
| IN2 | 1 | 接收車機OBDII模擬感測資料並儲存成記錄檔。 |
| IN3 | 1 | 接收路邊裝置影像並儲存成影片。 |
| IN4 | 1 | 車機、路邊裝置及伺服器透過Socket連線傳遞資料。 |
| IN5 | 1 | 網路連線透過Socket傳遞資料。 |

**系統外部介面:**

1. 需透過Socket連接車機、路邊裝置及伺服器。
2. 需使用於網路環境(如：WiFi, LAN, 3G, 4G)。
3. 需透過UART介面使車機介面溝通。

**系統內部介面:**

子計畫一：

車機及路邊裝置資料蒐集儲存介面。

網路連線傳輸介面。

使用者網頁服務介面。

子計畫二：

HDFS存取介面。

資料庫存取介面。

使用者資料存取介面。

子計畫三：

提供物聯網端點屬性加密開發套件(SDK)給子計畫二實作資料存取安全。

根據子計畫一提供之網路資訊建立VP-IoT。

提供子計畫四驗證樣本束是否經由授權的節點且是以經過共識決定的方式處理。

## 1.1測試範圍 (SCOPE OF TESTING)

本文件內容將依據系統需求規格書與系統設計文件，描述關於整合測試的相關計畫與內容。在確認本系統整合前，必須先確認所有的設計之子系統均能正確無誤的運作，因此著重於單元測試(Unit Test)、整合系統測試(Integration Test)及接受度測試(Acceptance Test)，並透過此文件之描述與實踐，達到順利進行測試工作之目的。

## 1.2接受準則 (ACCEPTANCE CRITERIA)

本測試計畫須滿足下列測試接受準則:

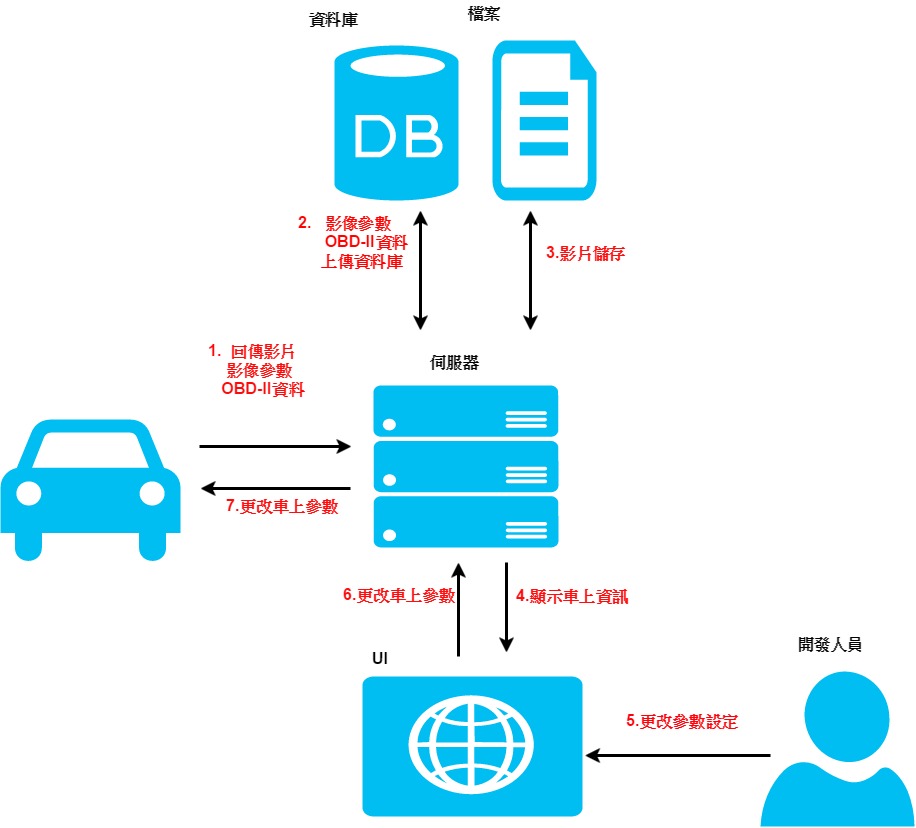
* 本計畫內所有系統需要對所有列為必要 ( Critical、Important、Desirable ) 之需求作完整測試。
* 測試程序需要依照本測試計畫所訂定的程序進行，所有測試結果需要能符合預期測試結果方能接

受。

* 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規定相同。

# 2 SECTION 2 TESTING ENVIRONMENT

下圖為本計畫進行測試的環境架構：



## 2.1硬體規格 (HARDWARE SPECIFICATION)

依據測試環境架構圖內容，進行測試之硬體規格說明，如下所示：

(1)桌上型電腦(伺服器端)

* 處理器：Intel(R)Core(TM) i5-4590 CPU@ 3.30GHz 3.30GHz。
* 記憶體：12 GB。
* 硬碟空間：1 TB。
* 作業系統：Windows 7 64 bit。

(2)工業電腦(車機及路邊裝置端)

* 處理器：Intel Atom Processor E3825 Dual Core SoC 1.33GHz。
* 記憶體：8 GB。
* 硬碟空間：1 TB。
* 作業系統：Ubuntu 16.04。

(3)筆記型電腦(工程人員端)

* 處理器：Intel(R)Core(TM) i5-4590 CPU@ 3.30GHz 3.30GHz。
* 記憶體：8 GB。
* 硬碟空間：750 GB。
* 作業系統：Windows 10 64 bit。

## 2.2軟體規格 (SOFTWARE SPECIFICATION)

依據測試環境內容，關於測試環境所需的軟體規格說明，如下所示：

* 伺服器端：Windows 7 64 bit與相關開發套件(如Java 1.8.0\_161等)。
* 車機及路邊裝置端：Ubuntu 16.04與相關開發套件(如Java 1.8.0\_161等)。
* 工程人員端：Windows 10 64 bit與網頁瀏覽器(如Google Chrome、Microsoft IE 11、Firefox等)。

## 2.3測試資料來源 (TEST DATA SOURCES)

關於測試所需的測試資料，如下所示：

* 實際道路駕駛影像。
* 路邊裝置影像。
* OBDII模擬器數據。

# 3 SECTION 3 TESTING SCHEDULE, PR OCEDURE, AND RESPONSIBILITY

## 3.1計畫測試時程 (TESTING SCHEDULE)

根據專案執行規劃書計畫書，測試時程107年1月起至107年5月止，詳細時程說明如下。

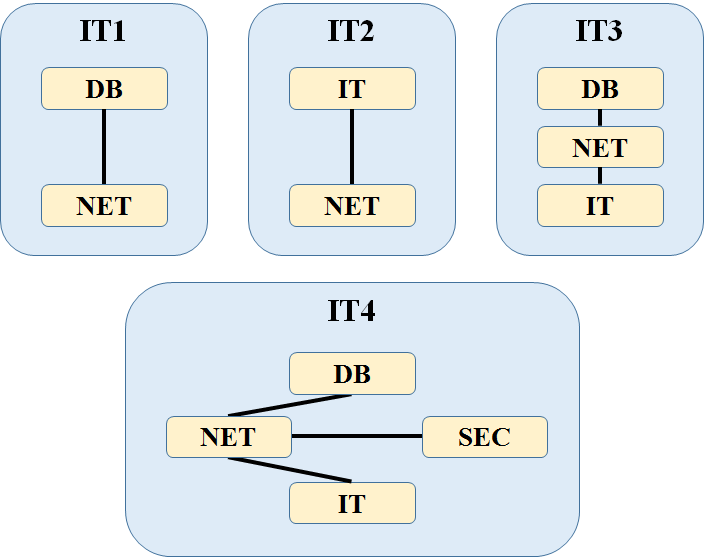
* 時程
  + 各種設備連線與串流測試(107/01/01 ~ 107/02/05)
  + 系統功能測試(107/02/05 ~ 107/03/10)
  + 系統效能測試(107/03/10 ~ 107/04/10)
* 查核點
  + 各子系統之內部元件整合測試(107/04/11)
  + 系統功能測試(107/04/20)
  + 系統效能測試(107/04/30)
  + 系統測試計畫書審查(107/05/15)

## 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整合測試 (Integration Testing)

基於需求規格報告書，在此本計畫著重於個子系統之間的整合測試與系統接受度測試。整合的順序為IT1🡪IT2🡪IT3🡪IT4。



## 3.3人員職責分配 (PERSONNEL RESPONSIBILITY ASSIGNMENT)

本計畫測試人員與工作項目

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 成員名單與編號對照表 | | | | | |
| 編號 | 姓名 | 編號 | 姓名 | 編號 | 姓名 |
| 01 | 陳朝烈教授 | 08 | 黃泰洲 | 15 | 張家榮 |
| 02 | 蘇維宗教授 | 09 | 連翊安 | 16 | 許登雄 |
| 03 | 陳朝鈞教授 | 10 | 莊旻哲 | 17 | 蔡政霖 |
| 04 | 林應傑 | 11 | 曾柏家 | 18 | 金建宇 |
| 05 | 許智偉 | 12 | 李昱興 | 19 | 吳明洋 |
| 06 | 王竹尉 | 13 | 王皓瑋 | 20 | 陳韋綸 |
| 07 | 廖柏洵 | 14 | 林昱明 | 21 | 鄒年澤 |

|  |  |
| --- | --- |
| Testing Activites | Personnal |
| IT1 | 01/ 04/ 05/ 08/ 11 |
| IT2 | 01/ 02/ 04/ 05/ 12/ 13/ 17 |
| IT3 | 01/ 03/ 06/ 07/ 09/ 11/ 12/ 13/14/ 16/ 19/ 21 |
| IT4 | 01/ 02/ 03/ 04/ 05/ 06/ 07/ 08/ 11/ 12/ 14/ 15/ 17/ 18/ 20 |
| AT1 | 01/ 05/ 07/ 15/ 16/ 17 |
| AT2 | 01/ 02/ 04/ 06/ 07/ 11/ 13 |
| AT3 | 01/ 02/ 03/ 04/ 05/ 08/ 09/ 10 |
| AT4 | 01/ 03/ 04/ 08/ 09/ 11/ 14/ 19/ |
| AT5 | 01/ 02/ 03/ 05/ 11/ 15/ 17/ 18/ 19/ 21 |
| AT6 | 01/ 02/ 03/ 04/ 05/ 06/ 07/ 08/ 11/ 12/ 13/ 14/ 17/ 18/ 20 |

## 3.3.1接受測試 (ACCEPTANCE TESTING)

本系統的接受度測試所列各子系統所有功能如下表所示:

|  |  |  |
| --- | --- | --- |
| **需求編號** | **優先順序** | **需求描述** |
| DB-1 | 1 | 使車機或路邊裝置登入並取得資訊。 |
| DB-2 | 1 | 提供使用者網頁伺服器服務。 |
| DB-3 | 1 | 送出要求至車機或路邊裝置。 |
| DB-4 | 1 | 顯示資訊或要求結果至網頁上。 |
| DB-5 | 1 | 接收使用者修改參數要求並送出至新車機或路邊裝置更新。 |

|  |  |  |
| --- | --- | --- |
| **需求編號** | **優先順序** | **需求描述** |
| NET-1 | 1 | 提供伺服器基本網路配置，可使車機搜尋並連接。 |
| NET-2 | 1 | 提供車機或路邊裝置基本網路配置，以連接伺服器。 |
| NET-3 | 1 | 車機可透過路邊裝置自動組成網路。 |
| NET-4 | 1 | 車機可自動判斷經過路邊裝置轉送或直接連接伺服器 |

|  |  |  |
| --- | --- | --- |
| **需求編號** | **優先順序** | **需求描述** |
| IT-1 | 1 | 擷取道路駕駛影像。 |
| IT-2 | 1 | 擷取OBDII感測資料。 |
| IT-3 | 1 | 自動連線至伺服器。 |
| IT-4 | 1 | 接收伺服器並回應或更新。 |

|  |  |  |
| --- | --- | --- |
| **需求編號** | **優先順序** | **需求描述** |
| SEC-1 | 1 | 產生CPABE屬性私密金鑰。 |
| SEC-2 | 1 | 將原始訊息以CPABE進行加密。 |
| SEC-3 | 1 | 將加密訊息以CPABE進行解密。 |

# 4 SECTION 4 TEST CASE

## 4.1 單元測試案例 (UNIT TESTING CASES)

**4.1. UT1 測試案例**

|  |  |
| --- | --- |
| Identification | UT1 |
| Name | 伺服器接受登入服務 |
| Tested target | DB |
| Reference | DB-1 |
| Severity | A |
| Instructions | 1. 伺服器接受車機或路邊裝置登入。 |
| Expected result | 1. 車機或路邊裝置正常登入伺服器。 |
| Cleanup | None |

**4.1. UT2 測試案例**

|  |  |
| --- | --- |
| Identification | UT2 |
| Name | 車機或路邊裝置可儲存影像 |
| Tested target | IT |
| Reference | IT-1 |
| Severity | A |
| Instructions | 1. 車機或路邊裝置可保留擷取之影像。 |
| Expected result | 1. 車機或路邊裝置擷取影像並存放。 |
| Cleanup | None |

**4.1. UT3 測試案例**

|  |  |
| --- | --- |
| Identification | UT3 |
| Name | 可觀看車機或路邊裝置支即時或歷史影像 |
| Tested target | IT |
| Reference | IT-1 |
| Severity | A |
| Instructions | 1. 可觀看車機或路邊裝置擷取之影像。 |
| Expected result | 1. 用戶可觀看車機或路邊裝置擷取。 |
| Cleanup | None |

**4.1. UT4 測試案例**

|  |  |
| --- | --- |
| Identification | UT4 |
| Name | 車機自動組成網路 |
| Tested target | NET |
| Reference | NET-3 |
| Severity | A |
| Instructions | 1. 車機可自動搜尋臨近車機或路邊裝置，並組成網路。 |
| Expected result | 1. 車機與臨近車機或路邊裝置自動組成網路，並互相交換訊息。 |
| Cleanup | None |

**4.1. UT5 測試案例**

|  |  |
| --- | --- |
| Identification | UT5 |
| Name | 確認Broker工作狀態 |
| Tested target | NET |
| Reference | NET-3 |
| Severity | A |
| Instructions | 1. 連線至自身。 2. 使Broker裝置發佈一則主題及訊息。 3. 使Broker裝置發佈該主題。 |
| Expected result | 1. 確認可連接上Broker。 2. 確認可發佈主題及訊息。 3. 確認訂閱主題後接收到對應訊息。 |
| Cleanup | None |

**4.1. UT6 測試案例**

|  |  |
| --- | --- |
| Identification | UT6 |
| Name | 發佈本地端資源清單 |
| Tested target | NET |
| Reference | NET-3 |
| Severity | A |
| Instructions | 1. 使本地端裝置連接至Broker。 2. 使本地端裝置發佈主題及訊息。 |
| Expected result | 1. 確認可連接上Broker。 2. 確認可發佈主題及訊息。 |
| Cleanup | None |

**4.1. UT7 測試案例**

|  |  |
| --- | --- |
| Identification | UT7 |
| Name | 訂閱本地端資源清單 |
| Tested target | NET |
| Reference | NET-3、NET-4 |
| Severity | A |
| Instructions | 1. 使本地端裝置連接至Broker。 2. 使本地端裝置訂閱主題。 |
| Expected result | 1. 確認可連接上Broker。 2. 確認訂閱主題後接收到對應訊息。 |
| Cleanup | None |

**4.1. UT8 測試案例**

|  |  |
| --- | --- |
| Identification | UT8 |
| Name | 切換Broker角色 |
| Tested target | NET |
| Reference | NET-3、NET-4 |
| Severity | A |
| Instructions | 1. 使接收到的資源清單進行比較。 2. 使比較程式執行完後產出新Broker名單。 |
| Expected result | 1. 確認可使接收到的資源清單進行比較。 2. 確認比較程式執行完後產出新Broker名單。 |
| Cleanup | None |

**4.1. UT9 測試案例**

|  |  |
| --- | --- |
| Identification | UT9 |
| Name | 隨裝置效能改變切換Broker角色 |
| Tested target | NET |
| Reference | NET-3、NET-4 |
| Severity | A |
| Instructions | 1. 使各裝置發佈自身資源清單。 2. 使各裝置中資源比較程式執行。 3. 比較程式執行完後產出新Broker角色。 4. 各裝置重新連線至新Broker角色進行資料交換發佈與訂閱。 |
| Expected result | 1. 確認可使各裝置發佈自身資源清單。 2. 確認使各裝置中資源比較程式執行。 3. 確認比較程式執行完後產出新Broker角色。 4. 確認各裝置重新連線至新Broker角色進行資料發佈與訂閱。 |
| Cleanup | None |

**4.1. UT10 測試案例**

|  |  |
| --- | --- |
| Identification | UT10 |
| Name | 影像來源輸入至FPGA平台 |
| Tested target | IT |
| Reference | IT-1 |
| Severity | A |
| Instructions | 1. FPGA平台接受影像來源輸入。 |
| Expected result | 1. CCD攝影機正常輸入影像至FPGA平台。 |
| Cleanup | None |

**4.1. UT11 測試案例**

|  |  |
| --- | --- |
| Identification | UT11 |
| Name | FPGA平台執行影像辨識 |
| Tested target | IT |
| Reference | IT-1 |
| Severity | A |
| Instructions | 1. FPGA平台接受影像來源進行影像辨識 |
| Expected result | 1. 行車影像正常在FPGA平台進行辨識 |
| Cleanup | None |

**4.1. UT12 測試案例**

|  |  |
| --- | --- |
| Identification | UT12 |
| Name | 使用CPABE產生私密金鑰 |
| Tested target | SEC |
| Reference | SEC-1 |
| Severity | A |
| Instructions | 1. 提供訊息加解密之私密金鑰。 |
| Expected result | 1. 私密金鑰正確產生。 |
| Cleanup | None |

**4.1. UT13 測試案例**

|  |  |
| --- | --- |
| Identification | UT13 |
| Name | 將未加密訊息使用CPABE進行加密 |
| Tested target | SEC |
| Reference | SEC-2 |
| Severity | A |
| Instructions | 1. 使訊息以密文方式傳遞。 |
| Expected result | 1. 訊息經過私密金鑰加密為密文。 |
| Cleanup | None |

**4.1. UT14 測試案例**

|  |  |
| --- | --- |
| Identification | UT14 |
| Name | 使用CPABE將已加密訊息進行解密 |
| Tested target | SEC |
| Reference | SEC-3 |
| Severity | A |
| Instructions | 1. 解析原始訊息。 |
| Expected result | 1. 將密文解密，顯示原始訊息。 |
| Cleanup | None |

## 4.2 整合測試案例 (INTEGRATION TESTING CASES)

**4.2.1 IT1 測試案例**

|  |  |
| --- | --- |
| Identification | IT1 |
| Name | 將伺服器公開於Internet提供車機連接 |
| Tested target | DB、NET |
| Reference | DB-1、NET-1 |
| Severity | A |
| Instructions | 1. 使伺服器公開至Internet。 |
| Expected result | 1. 確認可於Internet搜尋到伺服器。 2. 確認車機及路邊裝置可連線伺服器。 |
| Cleanup | None |

**4.2.2 IT2 測試案例**

|  |  |
| --- | --- |
| Identification | IT2 |
| Name | 將車機透過Internet，並連線至伺服器 |
| Tested target | IT、NET |
| Reference | IT-1、NET-2 |
| Severity | A |
| Instructions | 1. 車機可正常使用網路功能。 2. 車機可透過網路找到公開的伺服器，並進行連線。 |
| Expected result | 1. 車機可連接網際網路。 2. 車機可搜尋並連線至伺服器。 |
| Cleanup | None |

**4.2.3 IT3 測試案例**

|  |  |
| --- | --- |
| Identification | IT3 |
| Name | 於伺服器接收要求並送至車機取得回應 |
| Tested target | DB、NET、IT |
| Reference | DB-1、DB-3、DB-4、DB-5、NET-1、NET-2、IT-3  、IT-4 |
| Severity | A |
| Instructions | 1. 接收使用者觀看車機影片資訊或更新車機要求 2. 於伺服器送出要求至車機。 3. 於車機接收要求，並回傳結果至伺服器。 |
| Expected result | 1. 伺服器可接收使用者要求。 2. 伺服器可送出要求至車機。 3. 車機接收要求，並回應伺服器或更新。 |
| Cleanup | None |

**4.2.4 IT4 測試案例**

|  |  |
| --- | --- |
| Identification | IT4 |
| Name | 系統完整執行 |
| Tested target | DB、NET、IT、SEC |
| Reference | DB-1、DB-2、DB-3、DB-4、DB-5、NET-1、NET-2、NET-3、NET-4、IT-1、IT-2、IT-3、IT-4、SEC-1、SEC-2、SEC-3 |
| Severity | A |
| Instructions | 1. 完成系統整合。 2. 提供服務。 |
| Expected result | 1. 使完整系統開始運作。 |
| Cleanup | None |

## 4.3 接受測試案例 (ACCEPTANCE TESTING CASES)

**4.3.1 AT1 測試案例**

|  |  |
| --- | --- |
| Identification | AT1 |
| Name | 測試連線登入動作 |
| Tested target | DB、NET、IT |
| Reference | DB-1、NET-1、NET-2、IT-1 |
| Severity | A |
| Instructions | 1. 測試車機及路邊裝置與伺服器進行連線。 |
| Expected result | 1. 伺服器可取得車機資訊。 |
| Cleanup | None |

**4.3.2 AT2 測試案例**

|  |  |
| --- | --- |
| Identification | AT2 |
| Name | 測試車機及路邊裝置擷取影像及OBDII感測資料 |
| Tested target | IT |
| Reference | IT-1、IT-2 |
| Severity | A |
| Instructions | 1. 車機確實擷取影像並保存。 2. 車機確實擷取OBDII感測資料並保存。 |
| Expected result | 1. 於車機上查看保存之影像及感測資料。 |
| Cleanup | None |

**4.3.3 AT3 測試案例**

|  |  |
| --- | --- |
| Identification | AT3 |
| Name | 測試網頁伺服器運作 |
| Tested target | DB、NET、IT |
| Reference | DB-1、DB-2、DB-3、DB-4、NET-1、NET-2、IT-3、IT-4 |
| Severity | A |
| Instructions | 1. 網頁伺服器正常啟動。 2. 顯示車機或路邊裝置之資訊。。 |
| Expected result | 1. 使用者可以正常瀏覽網頁。 2. 使用者可以從網頁上查看指定車機或路邊裝置之資訊。 3. 使用者可透過網頁修改並更新車機或路邊裝置之參數。 |
| Cleanup | None |

**4.3.4 AT4 測試案例**

|  |  |
| --- | --- |
| Identification | AT4 |
| Name | 測試網頁可正常要求車機資訊及影像及送出更新車機要求 |
| Tested target | DB、NET、IT |
| Reference | DB-1、DB-2、DB-3、DB-4、DB-5、NET-1、NET-2、IT-3、IT-4 |
| Severity | A |
| Instructions | 1. 車機或路邊裝置之資訊及影像，於指定要求時，傳送至伺服器。 2. 可透過網頁修改參數並更新車機或路邊裝置 |
| Expected result | 1. 網頁顯示車機或路邊裝置之資訊或影像。 |
| Cleanup | None |

**4.3.5 AT5 測試案例**

|  |  |
| --- | --- |
| Identification | AT5 |
| Name | 測試車機與伺服器可處於不同網路下互相傳遞資料 |
| Tested target | DB、NET、IT |
| Reference | DB-1、DB-2、DB-3、DB-4、DB-5、NET-1、NET-2、IT-3、IT-4 |
| Severity | A |
| Instructions | 1. 車機與伺服器處於不同網路環境下，仍可互相傳遞資料。 |
| Expected result | 1. 伺服器可取得車機資訊或影像 |
| Cleanup | None |

**4.3.6 AT6 測試案例**

|  |  |
| --- | --- |
| Identification | AT6 |
| Name | 系統完整執行狀況 |
| Tested target | DB、NET、IT、SEC |
| Reference | DB-1、DB-2、DB-3、DB-4、DB-5、NET-1、NET-2、NET-3、NET-4、IT-1、IT-2、IT-3、IT-4、SEC-1、SEC-2、SEC-3 |
| Severity | A |
| Instructions | 1. 系統完整提供服務 |
| Expected result | 1. 使用者可操作網頁，並使用各項服務 |
| Cleanup | None |

# 5 TEST RESULT AND ANALYSIS

## 5.1 整合測試案例 (INTEGRATION TESTING CASES)

|  |  |  |
| --- | --- | --- |
| Test Case# | Results (PASS/ FAIL) | Comment |
| IT1 | PASS | 確認伺服器正常連線至Internet。 |
| IT2 | PASS | 確認車機正常連線至網路並可搜尋到伺服器。 |
| IT3 | PASS | 確認伺服器及車機連線、傳送要求、回應結果動作。 |
| IT4 |  |  |
| Rate | 75% |  |

## 5.2 接受測試案例 (ACCEPTANCE TESTING CASES)

|  |  |  |
| --- | --- | --- |
| Test Case# | Results (PASS/ FAIL) | Comment |
| AT1 | PASS | 車機或路邊裝置成功登入伺服器，並傳送自身資訊。 |
| AT2 | PASS | 查看車機或路邊裝置存放擷取之影像。 |
| AT3 | PASS | 網頁伺服器確實提供服務。 |
| AT4 | PASS | 確認車機及路邊裝置資訊顯示於網頁。 |
| AT5 | PASS | 確認伺服器可正常取得車機或路邊裝置之資訊，並可互相傳遞資料。 |
| AT6 |  |  |
| Rate | 83% |  |

# TRACEABILITY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subsystem Test Case | DB | NET | IT | SEC |
| IT1 | V | V |  |  |
| IT2 |  | V | V |  |
| IT3 | V | V | V |  |
| AT1 | V | V | V |  |
| AT2 |  |  | V |  |
| AT3 | V | V | V |  |
| AT4 | V | V | V |  |
| AT5 | V | V | V |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Test Case  requirement | IT1 | IT2 | IT3 | IT4 | AT1 | AT2 | AT3 | AT4 | AT5 | AT6 |
| DB-1 | V |  | V | V | V |  | V | V | V | V |
| DB-2 |  |  |  | V |  |  | V | V | V | V |
| DB-3 |  |  | V | V |  |  | V | V | V | V |
| DB-4 |  |  | V | V |  |  | V | V | V | V |
| DB-5 |  |  | V | V |  |  |  | V | V | V |
| NET-1 | V |  | V | V | V |  | V | V | V | V |
| NET-2 |  | V | V | V | V |  | V | V | V | V |
| IT-1 |  | V |  | V | V | V |  |  |  | V |
| IT-2 |  |  |  | V |  | V |  |  |  | V |
| IT-3 |  |  | V | V |  |  | V | V | V | V |
| IT-4 |  |  | V | V |  |  | V | V | V | V |
| SEC-1 |  |  |  | V |  |  |  |  |  | V |
| SEC-2 |  |  |  | V |  |  |  |  |  | V |
| SEC-3 |  |  |  | V |  |  |  |  |  | V |

# 附錄一

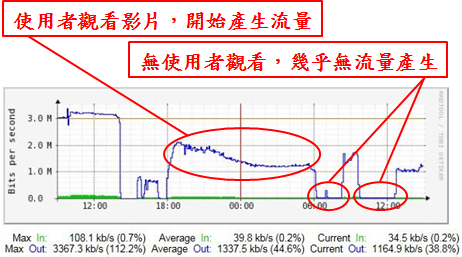
觀看路邊裝置直播影像：



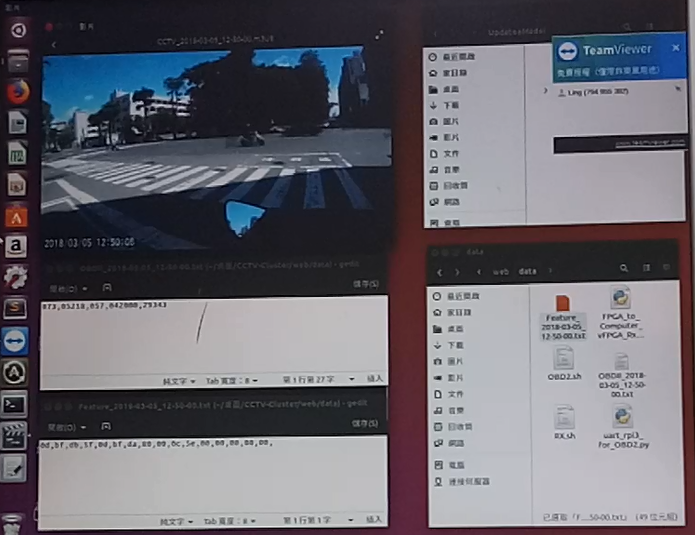
觀看路邊裝置歷史影像：



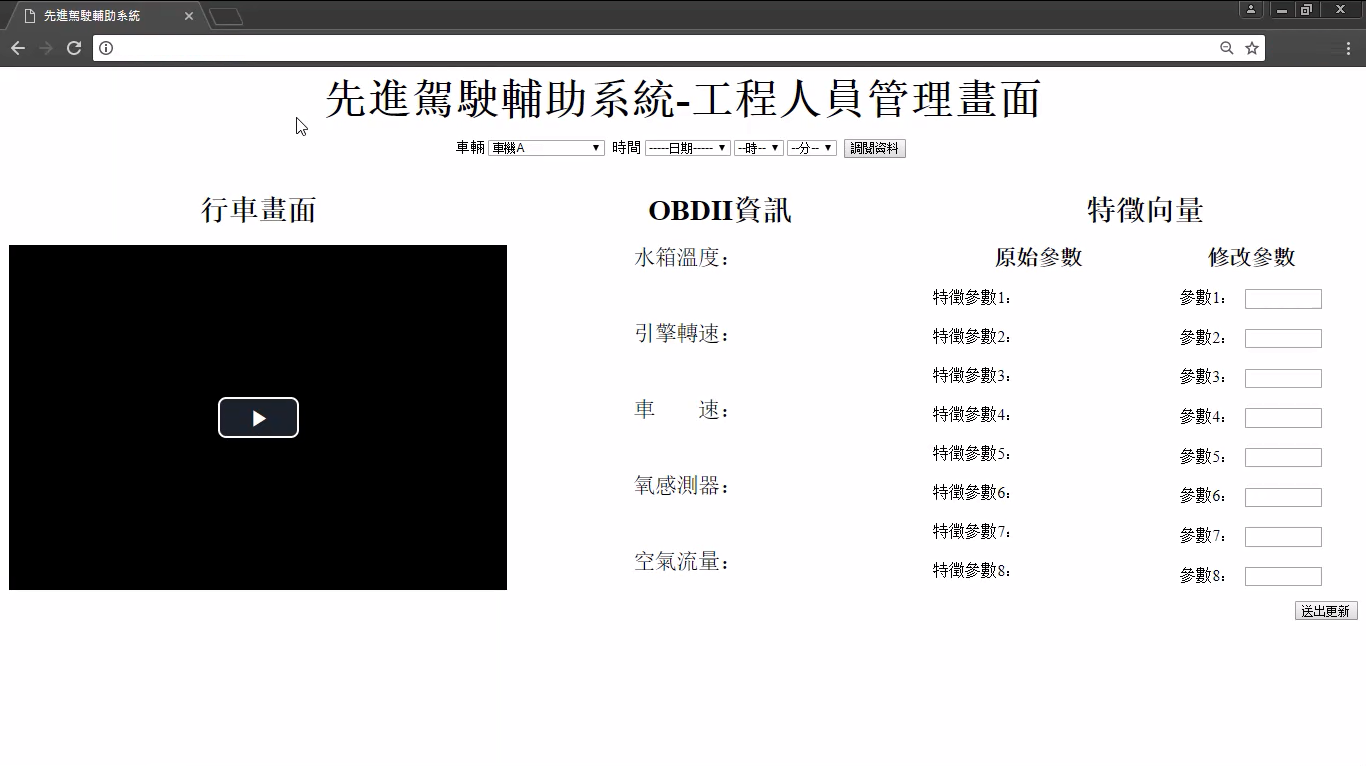
車機及路邊裝置實際使用網路流量：



車機上查看影像、OBDII資料及特徵參數：



工程人員端-網頁伺服器基本資訊：



工程人員端-網頁伺服器查看車機資訊：

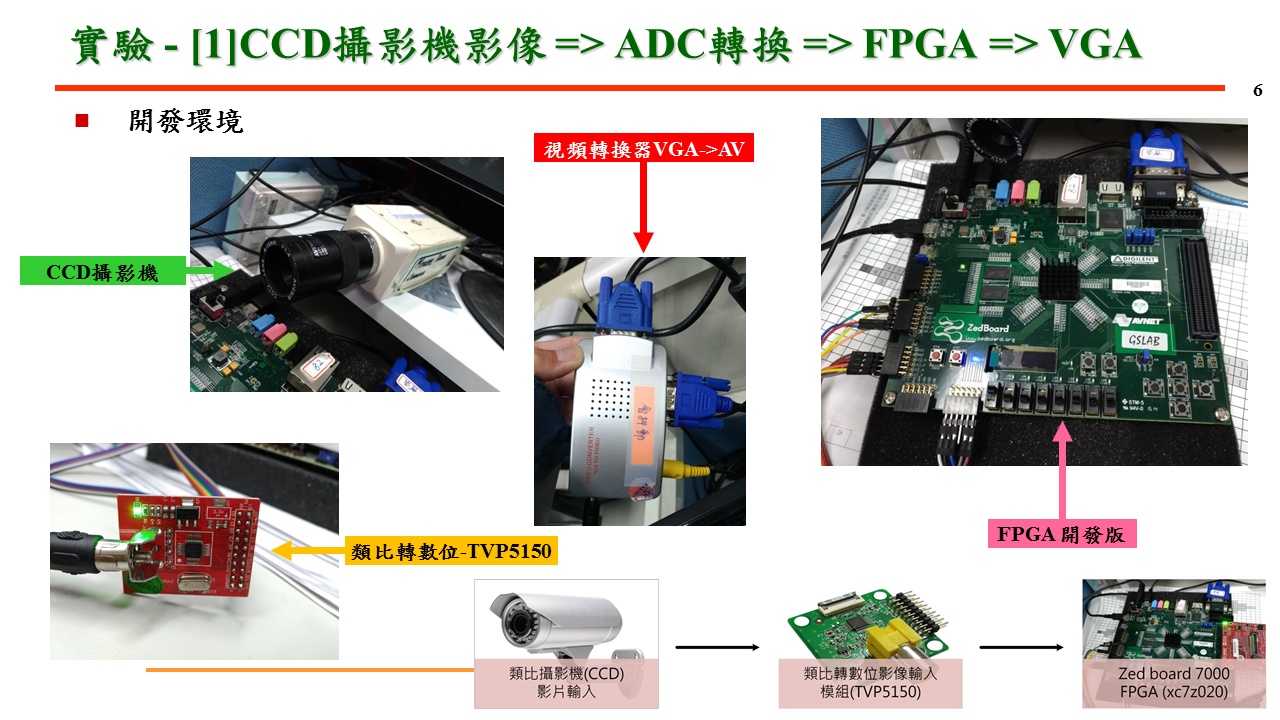


工程人員端-網頁伺服器送出更新至車機：



# 附錄二

影像來源輸入至FPGA平台:



CCD攝影機正常輸入影像至FPGA平台

FPGA平台執行影像辨識-即時影像辨識出畫面中的機車

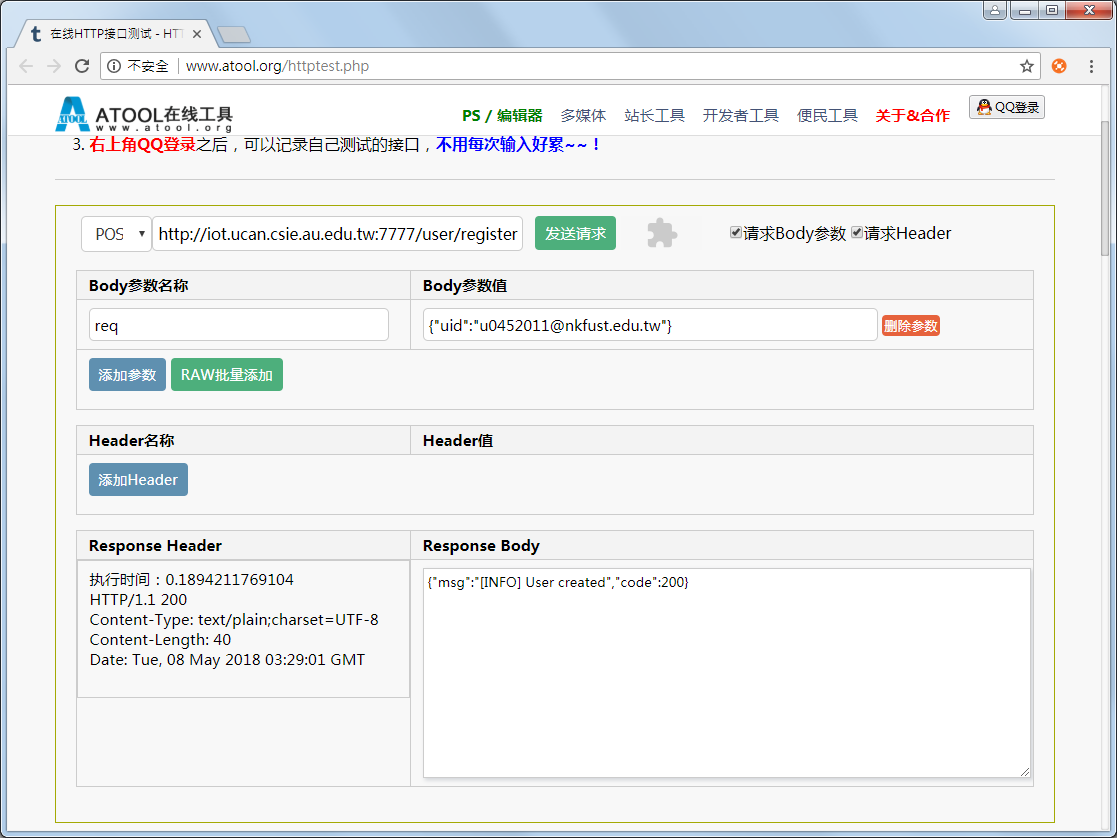


FPGA平台執行影像辨識-即時影像辨識出畫面中的汽車

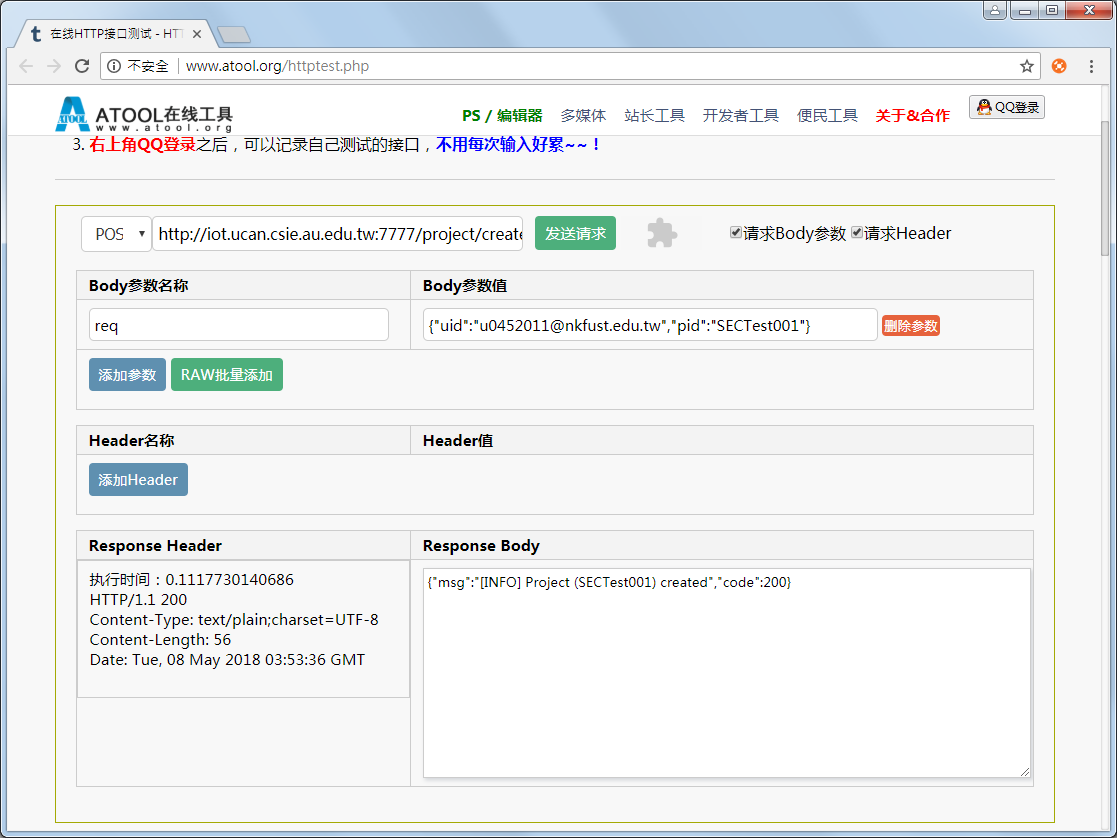


# 附錄三

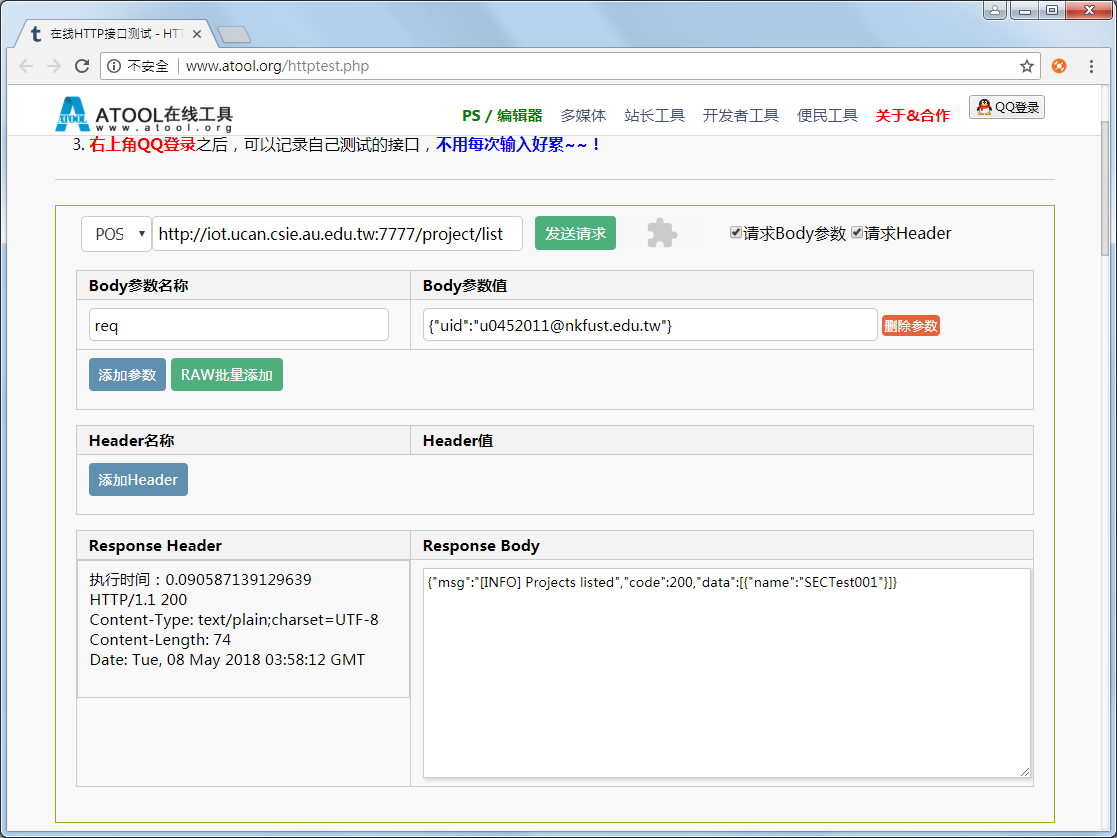
密文政策屬性加密(CPABE)-建立使用者



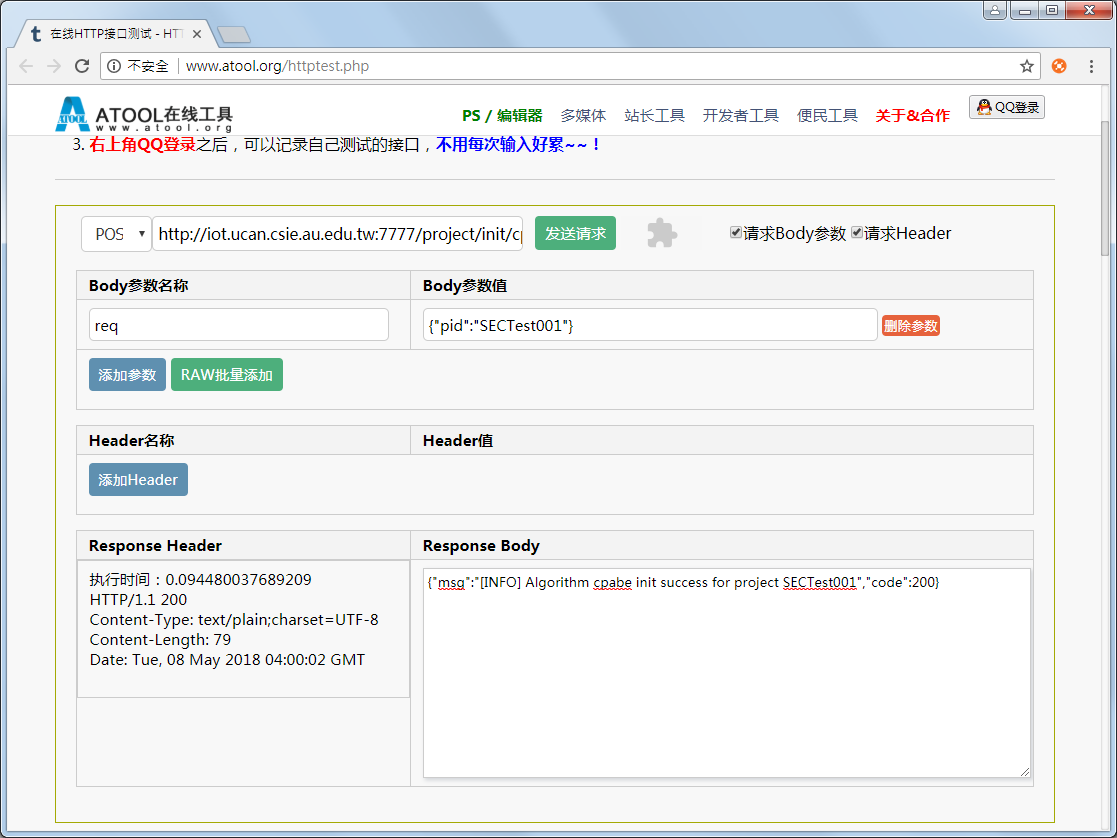
密文政策屬性加密(CPABE)-建立專案



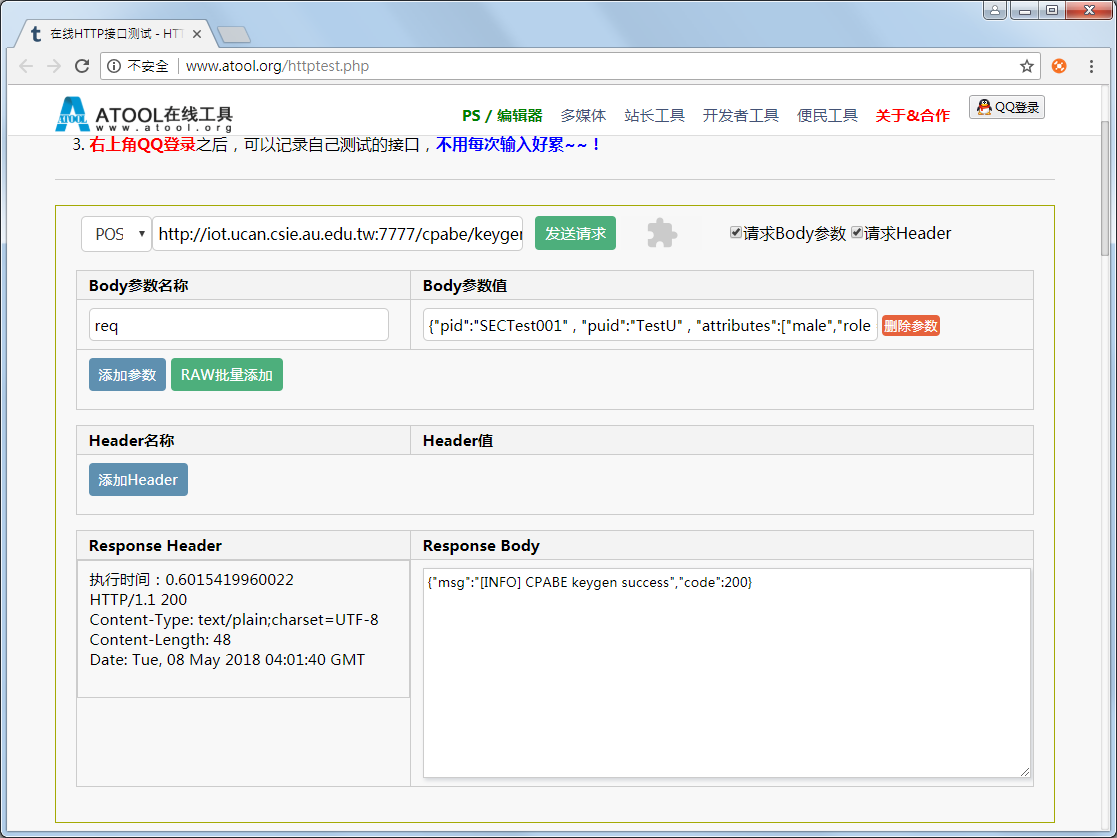
密文政策屬性加密(CPABE)-查看使用者之專案



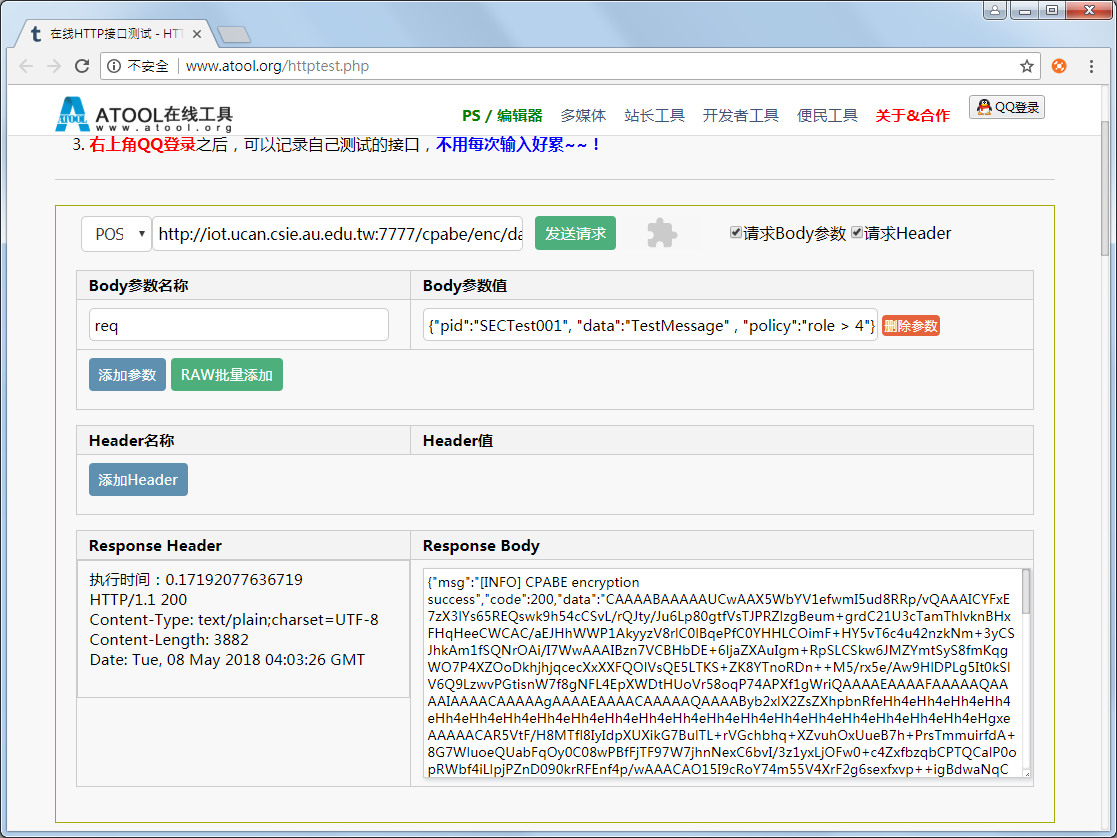
密文政策屬性加密(CPABE)-初始化演算法



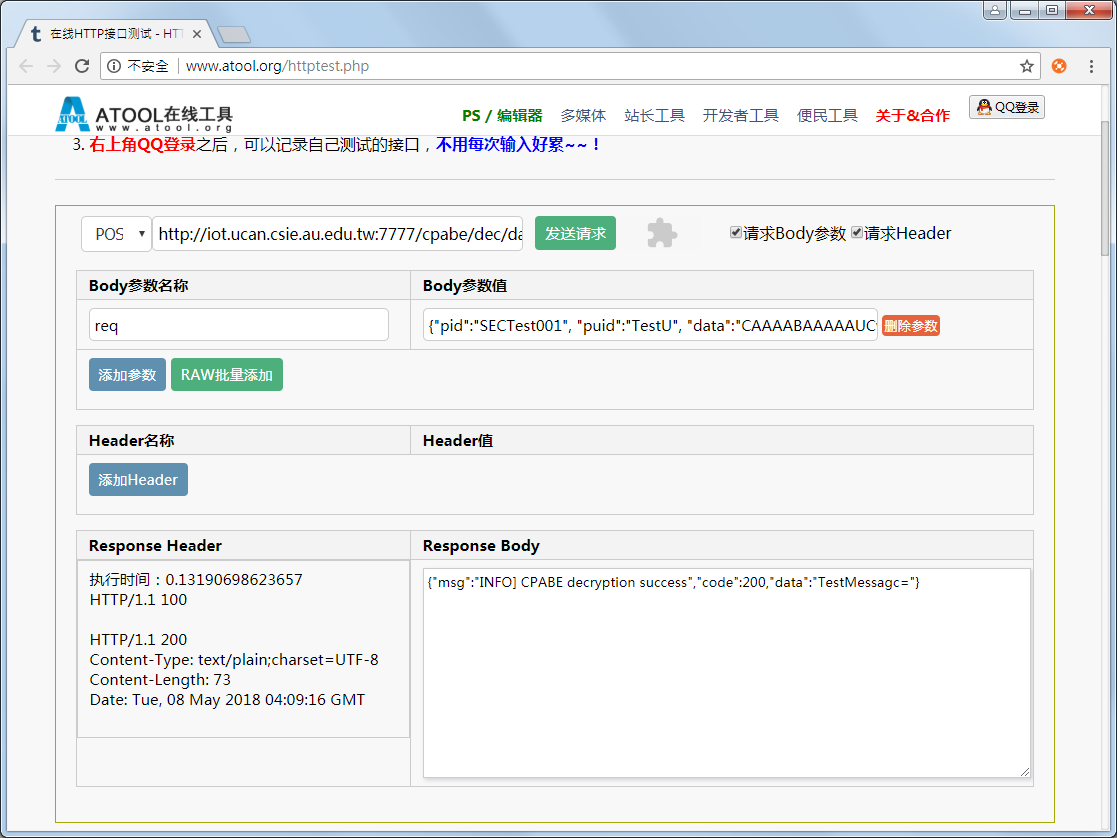
密文政策屬性加密(CPABE)-產生CPABE屬性私密金鑰



密文政策屬性加密(CPABE)-使用CPABE加密資料，測試資料為TestMessage



密文政策屬性加密(CPABE)- 使用CPABE解密資料



# 子計畫三-測試報告

目錄

[目錄 34](#_Toc513547518)

[圖目錄 36](#_Toc513547519)

[表目錄 37](#_Toc513547520)

[版本更變記錄 38](#_Toc513547521)

[1. 介紹 39](#_Toc513547522)

[1.1. 測試涵蓋範圍 39](#_Toc513547523)

[1.2. 測試接受準則 39](#_Toc513547524)

[2. 測試環境 40](#_Toc513547525)

[2.1. 操作環境 40](#_Toc513547526)

[2.2. 硬體規格 40](#_Toc513547527)

[2.3. 軟體規格 41](#_Toc513547528)

[2.4. 測試資料 41](#_Toc513547529)

[3. 測試時程、程序、與責任歸屬 42](#_Toc513547530)

[3.1. 測試時程 42](#_Toc513547531)

[3.2. 測試程序 42](#_Toc513547532)

[3.2.1. 子計畫驗證 42](#_Toc513547533)

[3.3. 測試人員與責任歸屬 42](#_Toc513547534)

[4. 測試案例 43](#_Toc513547535)

[4.1. 整合測試案例 43](#_Toc513547536)

[4.1.1. FT01功能測試案例 43](#_Toc513547537)

[4.1.2. FT02功能測試案例 43](#_Toc513547538)

[4.1.3. FT03功能測試案例 44](#_Toc513547539)

[4.1.4. PT01效能測試案例 44](#_Toc513547540)

[4.1.5. PT02效能測試案例 45](#_Toc513547541)

[4.1.6. PT03效能測試案例 45](#_Toc513547542)

[5. 測試結果與分析 47](#_Toc513547543)

[5.1. 功能測試結果與分析 47](#_Toc513547544)

[5.2. 效能測試結果與分析 47](#_Toc513547545)

[附錄A: 追溯矩陣 49](#_Toc513547546)

**圖目錄**

[圖 1. 本計畫擬開發系統之架構圖(規劃三年完成) 38](#_Toc513547547)

[圖 2. 測試環境部署圖 39](#_Toc513547548)

[圖 4. 資料量與加解密時間的關係圖 46](#_Toc513547549)

[圖 5. 存取政策中屬性故數與加解密時CPU使用率關係圖 46](#_Toc513547550)

[圖 6. 資料量與IoT Device本地解密與卸載解密時間的關係圖 47](#_Toc513547551)

# 表目錄

[表格 1. 硬體規格 39](#_Toc513547552)

[表格 2. 測試人員角色與責任 41](#_Toc513547553)

[表格 3. TP Device可以執行CP-ABE功能測試案例說明 42](#_Toc513547554)

[表格 4. IoT Device可以執行CP-ABE功能測試案例說明 42](#_Toc513547555)

[表格 5. IoT Device卸載CP-ABE加解密功能 43](#_Toc513547556)

[表格 6. 資料量對加解密效能的影響 43](#_Toc513547557)

[表格 8. 存取政策中屬性數量對加解密效能的影響 44](#_Toc513547558)

[表格 8.資料量對於IoT Device本地解密與卸載解密效能的影響 44](#_Toc513547559)

[表格 9. 系統模組與測試案例的追溯矩陣 48](#_Toc513547560)

# 版本更變記錄

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **修改日期** | **版本** | **文件狀態** | **描述** | **負責人** |
| 2018/05/07 | 1.0 | Release | 測試報告完稿確認 | 蘇維宗 |
| 2018/04/17 | 0.2 | Beta | 加入效能測試結果 | 陳韋丞 |
| 2017/12/01 | 0.1 | Draft | 初稿 | 陳韋丞 |

1. **介紹**

本子計畫106年度主要的研究議題是如何讓資源有限的物聯網裝置(即車機)能夠將複雜的運算，例如屬性加密技術(Attribute-Based Encryption)，卸載到鄰近可信賴的裝置進行運算。為了提高行動裝置運算卸載的安全性，我們提出了一個可以從聯網裝置過去的行為來評估其可信賴度來選擇運算卸載的目標。根據運算卸載標的歷史行為(Historical Behavior of Thing)選擇運算卸載目標的優點在於可以透過數據分析來量化信賴度以提高運算卸載的安全性。

本測試計畫主要是對圖 1中的依據信賴值評估之安全卸載方法(2.0 Secure Offloading under TRUst Evaluation，簡稱SOTRUE)軟體模組進行功能與效能測試。本子計畫所開發之運算卸載軟體原始碼(beebit-seco-api專案)已發布在GitHub平台上提供下載測試與使用，專案網址為https://github.com/ucanlab/beebit-seco-api。



圖 1. 本計畫擬開發系統之架構圖(規劃三年完成)

* 1. 測試涵蓋範圍

本文件內容將依據系統需求規格書與系統設計文件，描述關於整合測試的相關計畫與內容。在確認本系統整合前，必須先確認所有的設計之子系統均能正確無誤的運作，因此著重於整合系統測試(Integration Test)及接受測試(Acceptance Test)，並透過此文件之描述與實踐，達到順利進行測試工作之目的。

* 1. 測試接受準則

本測試計劃需要滿足下列的測試接受準則：

* 本系統需要對所有列為必要(Critical、Important、Desirable)之需求作完整測試。
* 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預期測試結果方能接受。
* 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規定相同。

1. **測試環境**
   1. 操作環境

本文件主要測試IoT Device (以Raspberry Pi 3模擬)將密文政策屬性加密(CP-ABE)卸載至Trust and Power Device (TP Device)執行的功能正確性與效能。圖 2為測試環境部署圖，Device將資料以CP-ABE加密後透過MQTT通訊協定傳送給IoT Device。IoT Device因為運算能力不足將解密運算卸載到TP Device進行運算。為了確保資料的保密性，TP Device只會降低存取政策內的屬性數量而無法得知明文的內容。接著，TP Device將轉換存取政策的密文回傳給IoT Device。最後，因為密文中存取政策的屬性數量降低，所以IoT Device可以更有效率地進行解密。

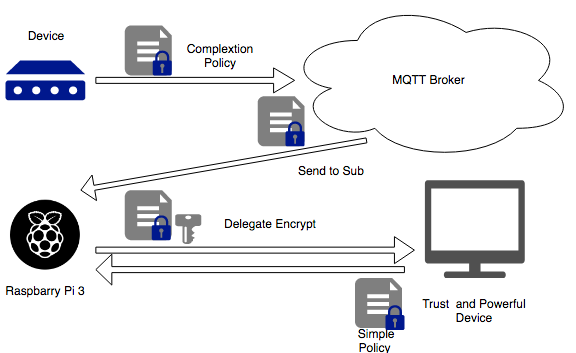


圖 2. 測試環境部署圖

* 1. 硬體規格

依據測試環境內容，關於測試環境所需的硬體規格說明，如表格 1所示:

表格 1. 硬體規格

|  |  |
| --- | --- |
| **TP Device / PC** | |
| **CPU** | Intel(R)Core(TM) i5-4200H CPU@ 2.80GHz 2.79GHz |
| **RAM** | 8.00 GB |
| **System type** | 64 bits |
| **IoT Device / Raspberry Pi 3** | |
| **CPU** | ARM Cortex-A7 (900 MHz) |
| **RAM** | 1 GB |
| **System type** | 64 bits |

* 1. 軟體規格

依據測試環境內容，關於測試環境所需的軟體規格說明，如下所示:

* Linux (64 bits)與相關開發套件(如gcc、make等)
* 基本函式庫套件，包含m4、flex、bison、libssl-dev、libgmp-dev(>4.0.0)與glib(>2.0.0)
* 屬性加密函式庫套件(libpbc、libbswabe、與cpabe)
* 本計畫開發之函式庫套件(libcpabe)
  1. 測試資料

測試資料為字串。字串的內容與大小另於測試案例描述。

1. **測試時程、程序、與責任歸屬**
   1. 測試時程

根據專案執行規劃書計畫書，測試時程107年3月起至107年5月止，詳細時程說明如下。

* 時程
  + 各子功能之內部元件整合測試(107/2/26 ~ 107/3/11)
  + 系統功能測試(107/3/12 ~ 107/4/8)
  + 系統效能測試(107/4/9 ~ 107/4/22)
* 查核點
  + 各子功能之內部元件整合測試確認(107/3/12)
  + 系統功能測試確認(107/4/8)
  + 系統效能測試確認(107/4/22)
  1. 測試程序
     1. 子計畫驗證

各子功能之內部元件測試，由各子系統開發負責人員完成，在此我們著重於所有子功能完成後之整合測試。

* 1. 測試人員與責任歸屬

表格 2. 測試人員角色與責任

|  |  |  |
| --- | --- | --- |
| **Testing Cases** | **Testing Target** | **Personnel** |
| FT01 | IoT Device加解密 | 陳韋丞 |
| FT02 | TP Device加解密 | 陳韋丞 |
| FT03 | IoT Device卸載解密 | 陳韋丞 |
| PT01 | 資料量對加解密效能的影響 | 魏祥宇 |
| PT02 | 存取政策內屬性個數對加解密謝能的影響 | 魏祥宇 |
| PT03 | 資料量對IoT Device本地解密與卸載解密的效能影響 | 魏祥宇 |

1. **測試案例**
   1. 整合測試案例
      1. FT01功能測試案例

**目的:** 驗證TP Device可以執行CP-ABE加解密功能且獲得正確結果。

表格 3. TP Device可以執行CP-ABE功能測試案例說明

|  |  |
| --- | --- |
| **Identification** | FT01 |
| **Name** | 驗證TP Device可以執行CP-ABE加解密功能 |
| **Assumption** | 函式庫libcpabe-01.a已整合到PC且功能正常 |
| **Pre-condition** | 已產生所有需要之金鑰 |
| **Target** | 呼叫ct = enc(pt)函式能夠正確加密明文pt並產生密文ct  呼叫pt = dec(ct)函式能夠正確解密密文ct並產生明文pt |
| **Test Object** | ct = enc(公開金鑰路徑, BASE64編碼明文字串, 存取政策)  pt = dec(公開金鑰路徑, 私密金鑰路徑, BASE64編碼密文字串) |
| **Severity** | Critical |
| **Test Source** | TS 1. 對”Hello”進行BASE64編碼產生的BASE64字串(pt) |
| **Instructions** | Step 1. 執行ct = enc(pt)  Step 2. 執行pt = dec(ct)  Step 3. 對pt進行BASE64解碼  Step 4. 確認解碼後的字串是否為Hello |
| **Test Result** | TR 1. 解碼後的字串為Hello [SUCCESS] |

* + 1. FT02功能測試案例

**目的:** 驗證IoT Device可以執行CP-ABE加解密功能且獲得正確結果。

**表格 4. IoT Device可以執行CP-ABE功能測試案例說明**

|  |  |
| --- | --- |
| **Identification** | FT02 |
| **Name** | 驗證IoT Device可以執行CP-ABE加解密功能 |
| **Assumption** | 函式庫libcpabe-01.a已整合到Raspberry Pi 3且功能正常 |
| **Pre-condition** | 已產生所有需要之金鑰 |
| **Target** | 呼叫ct = enc(pt)函式能夠正確加密明文pt並產生密文ct  呼叫pt = dec(ct)函式能夠正確解密密文ct並產生明文pt |
| **Test Object** | ct = enc(公開金鑰路徑, BASE64編碼明文字串, 存取政策)  pt = dec(公開金鑰路徑, 私密金鑰路徑, BASE64編碼密文字串) |
| **Severity** | Critical |
| **Test Source** | TS 1. 對”Hello”進行BASE64編碼產生的BASE64字串(pt) |
| **Instructions** | Step 1. 執行ct = enc(pt)  Step 2. 執行pt = dec(ct)  Step 3. 對pt進行BASE64解碼  Step 4. 確認解碼後的字串是否為Hello |
| **Test Result** | TR 1. 解碼後的字串為Hello [SUCCESS] |

* + 1. FT03功能測試案例

**目的:** 驗證IoT Device可以將CP-ABE加解密功能卸載到TP Device運算且獲得正確結果。

表格 5. IoT Device卸載CP-ABE加解密功能

|  |  |
| --- | --- |
| **Identification** | FT03 |
| **Name** | IoT Device可以卸載CP-ABE加解密功能 |
| **Assumption** | 函式庫libcpabe-01.a已整合到PC且功能正常  beebit-seco網頁服務在TP Device執行且功能正常 |
| **Pre-condition** | 已產生所有需要之金鑰 |
| **Target** | IoT Device呼叫TP Device上的/cpabe/enc/data服務進行加密卸載  IoT Device呼叫TP Device上的/cpabe/dec/data服務進行解密卸載 |
| **Test Object** | /cpabe/enc/data  /cpabe/dec/data |
| **Severity** | Critical |
| **Test Source** | TS 1. 對”Hello”進行BASE64編碼產生的BASE64字串(pt) |
| **Instructions** | Step 1. IoT Device呼叫TP Device上的/cpabe/enc/data並以pt為參數，TP Device加密後回傳密文ct  Step 2. IoT Device呼叫TP Device上的/cpabe/dec/data並以ct為參數，TP Device解密後回傳明文pt  Step 3. 對pt進行BASE64解碼  Step 4. 確認解碼後的字串是否為Hello |
| **Test Result** | TR 1. 解碼後的字串為Hello [SUCCESS] |

* + 1. PT01效能測試案例

**目的：**測試資料量對CP-ABE加解密效能的影響。

表格 6. 資料量對加解密效能的影響

|  |  |
| --- | --- |
| **Identification** | PT01 |
| **Name** | 測試資料量對CP-ABE加解密效能的影響 |
| **Assumption** | 函式庫libcpabe-01.a已整合到PC與Raspberry Pi 3且功能正常 |
| **Pre-condition** | 已產生所有需要之金鑰 |
| **Target** | 呼叫ct = enc(pt)函式能夠正確加密明文pt並產生密文ct  呼叫pt = dec(ct)函式能夠正確解密密文ct並產生明文pt |
| **Test Object** | ct = enc(公開金鑰路徑, BASE64編碼明文字串, 存取政策)  pt = dec(公開金鑰路徑, 私密金鑰路徑, BASE64編碼密文字串) |
| **Severity** | Critical |
| **Test Source** | TS 1. 10 KB的資料/1個屬性的存取政策 TS 2. 50 KB的資料/1個屬性的存取政策  TS 3. 100 KB的資料/1個屬性的存取政策 TS 4. 1000 KB的資料/1個屬性的存取政策  TS 5. 5000 KB的資料/1個屬性的存取政策  TS 6. 10000 KB的資料/1個屬性的存取政策 |
| **Instructions** | Step 1. 在IoT Device上分別從TS1至TS6執行ct = enc(pt)並記錄時間  Step 2. 在IoT Device上分別從TS1至TS6執行pt = dec(ct)並記錄時間  Step 3. 在TP Device上分別從TS1至TS6執行ct = enc(pt)並記錄時間  Step 4. 在TP Device上分別從TS1至TS6執行pt = dec(ct)並記錄時間 |
| **Test Result** | 根據實驗結果繪製資料量與加解密時間的關係圖 |

* + 1. PT02效能測試案例

**目的：**測試存取政策中屬性數量對CP-ABE加解密效能的影響。

表格 8. 存取政策中屬性數量對加解密效能的影響

|  |  |
| --- | --- |
| **Identification** | PT02 |
| **Name** | 測試存取政策中屬性數量對CP-ABE加解密效能的影響 |
| **Assumption** | 函式庫libcpabe-01.a已整合到PC與Raspberry Pi 3且功能正常 |
| **Pre-condition** | 已產生所有需要之金鑰 |
| **Target** | 呼叫ct = enc(pt)函式能夠正確加密明文pt並產生密文ct  呼叫pt = dec(ct)函式能夠正確解密密文ct並產生明文pt |
| **Test Object** | ct = enc(公開金鑰路徑, BASE64編碼明文字串, 存取政策)  pt = dec(公開金鑰路徑, 私密金鑰路徑, BASE64編碼密文字串) |
| **Severity** | Critical |
| **Test Source** | TS 1. 10個屬性的存取政策/1000KB的資料 TS 2. 20個屬性的存取政策/1000KB的資料  TS 3. 20個屬性的存取政策/1000KB的資料 |
| **Instructions** | Step 1. 在IoT Device上分別從TS1至TS3執行ct = enc(pt)並記錄CPU使用率  Step 2. 在IoT Device上分別從TS1至TS3執行pt = dec(ct)並記錄CPU使用率  Step 3. 在TP Device上分別從TS1至TS3執行ct = enc(pt)並記錄CPU使用率  Step 4. 在TP Device上分別從TS1至TS3執行pt = dec(ct)並記錄CPU使用率 |
| **Test Result** | 根據實驗結果繪製存取政策中屬性數量與加解密時CPU使用率的關係圖 |

* + 1. PT03效能測試案例

**目的：**測試資料量對於IoT Device本地解密與卸載解密效能的影響。

表格 8.資料量對於IoT Device本地解密與卸載解密效能的影響

|  |  |
| --- | --- |
| **Identification** | PT03 |
| **Name** | 資料量對於IoT Device本地解密與卸載解密效能的影響 |
| **Assumption** | 函式庫libcpabe-01.a已整合到PC與Raspberry Pi 3且功能正常 |
| **Pre-condition** | 已產生所有需要之金鑰 |
| **Target** | 呼叫ct = enc(pt)函式能夠正確加密明文pt並產生密文ct  呼叫pt = dec(ct)函式能夠正確解密密文ct並產生明文pt  IoT Device呼叫TP Device上的/cpabe/enc/data服務進行加密卸載  IoT Device呼叫TP Device上的/cpabe/dec/data服務進行解密卸載 |
| **Test Object** | ct = enc(公開金鑰路徑, BASE64編碼明文字串, 存取政策)  pt = dec(公開金鑰路徑, 私密金鑰路徑, BASE64編碼密文字串)  /cpabe/enc/data  /cpabe/dec/data |
| **Severity** | Critical |
| **Test Source** | TS 1. 1000 KB的資料/30個屬性的存取政策 TS 2. 5000KB的資料/30個屬性的存取政策  TS 3. 10000 KB的資料/30個屬性的存取政策 |
| **Instructions** | 本地解密  Step 1. 在IoT裝置上分別對TS1至T3執行pt = dec(ct)並記錄時間為本地解密的時間  卸載解密  Step 2. IoT Device呼叫TP Device上的/cpabe/dec/data並分別對TS1至T3為參數並記錄時間。  Step 3. 在TP Device上分別對TS1至TS3執行pt = dec(ct)並記錄時間  Step 4. 在TP Device上分別對TS1至TS3解密後的pt執行ct = enc(pt)並在存取政策中止加入一個屬性並記錄時間。  Step 5.TP Device將ct回傳給確IoT Device並記錄時間  Step 6. IoT Device對ct執行pt = dec(ct)並記錄時間  Step 7. 將Step 2-6的時間累計為卸載解密的時間 |
| **Test Result** | 根據實驗結果繪製資料量對於IoT Device本地解密與卸載解密時間的關係圖 |

1. **測試結果與分析**
   1. 功能測試結果與分析

|  |  |  |
| --- | --- | --- |
| **Test Case** | **Result (Pass / Fail)** | **Comment** |
| FT01 | Pass | 無 |
| FT02 | Pass | 無 |
| FT03 | Pass | 無 |
| **Rate** | 100% |  |

* 1. 效能測試結果與分析

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case** | **Expected Result** | **Test Result** | **Comment** |
| PT01 | N/A | Pass | 詳細測試結果請參閱圖 3  IoT Device與TP Device效能差了將近4倍 |
| PT02 | N/A | Pass | 詳細測試結果請參閱圖 4  IoT Device在屬性數量高時CPU使用率過高可能影響其它工作的正常運行 |
| PT03 | N/A | Pass | 詳細測試結果請參閱圖 5  資料量太大時因為傳輸時間太長導致卸載解密時間反而更長 |

一張含有 文字, 地圖 的圖片

描述是以非常高的可信度產生

圖 4. 資料量與加解密時間的關係圖

一張含有 螢幕擷取畫面 的圖片

描述是以非常高的可信度產生

圖 5. 存取政策中屬性故數與加解密時CPU使用率關係圖

一張含有 螢幕擷取畫面 的圖片

描述是以非常高的可信度產生

圖 6. 資料量與IoT Device本地解密與卸載解密時間的關係圖

**附錄A: 追溯矩陣**

表格 9. 系統模組與測試案例的追溯矩陣

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Test Cases  Module | FT01 | FT02 | FT03 | PT01 | PT02 | PT03 |
| 2.1 Security Measure Offloading | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ |
| 2.2 Statistical Device-Behavior Trust Evaluation |  |  | ◎ |  |  | ◎ |