

# 科技部工程司資訊安全實務研發專案期末成果展

## 總計畫：先進駕駛輔助系統之雲端輔助設計優化

### 子計畫三：植基於免疫系統之安全的物聯網應用開發方法 - 以先進駕駛輔助系統為例 An Immune System based Approach to Develop Secure IoT Applications using Advanced Driver Assistant Systems as a Case Study

計畫執行單位：真理大學 資訊工程學系(所)  
子計畫主持人：蘇維宗 助理教授  
計畫編號：MOST 105-2221-E-156-004

總計畫主持人：國立高雄第一科技大學 陳朝烈 教授  
計畫參與人員(碩士級)：碩士班：李念哲、陳韋丞  
計畫參與人員(學士級)：魏祥宇、蔡鎧澤、賴英綸、盧思璇

#### 計畫摘要

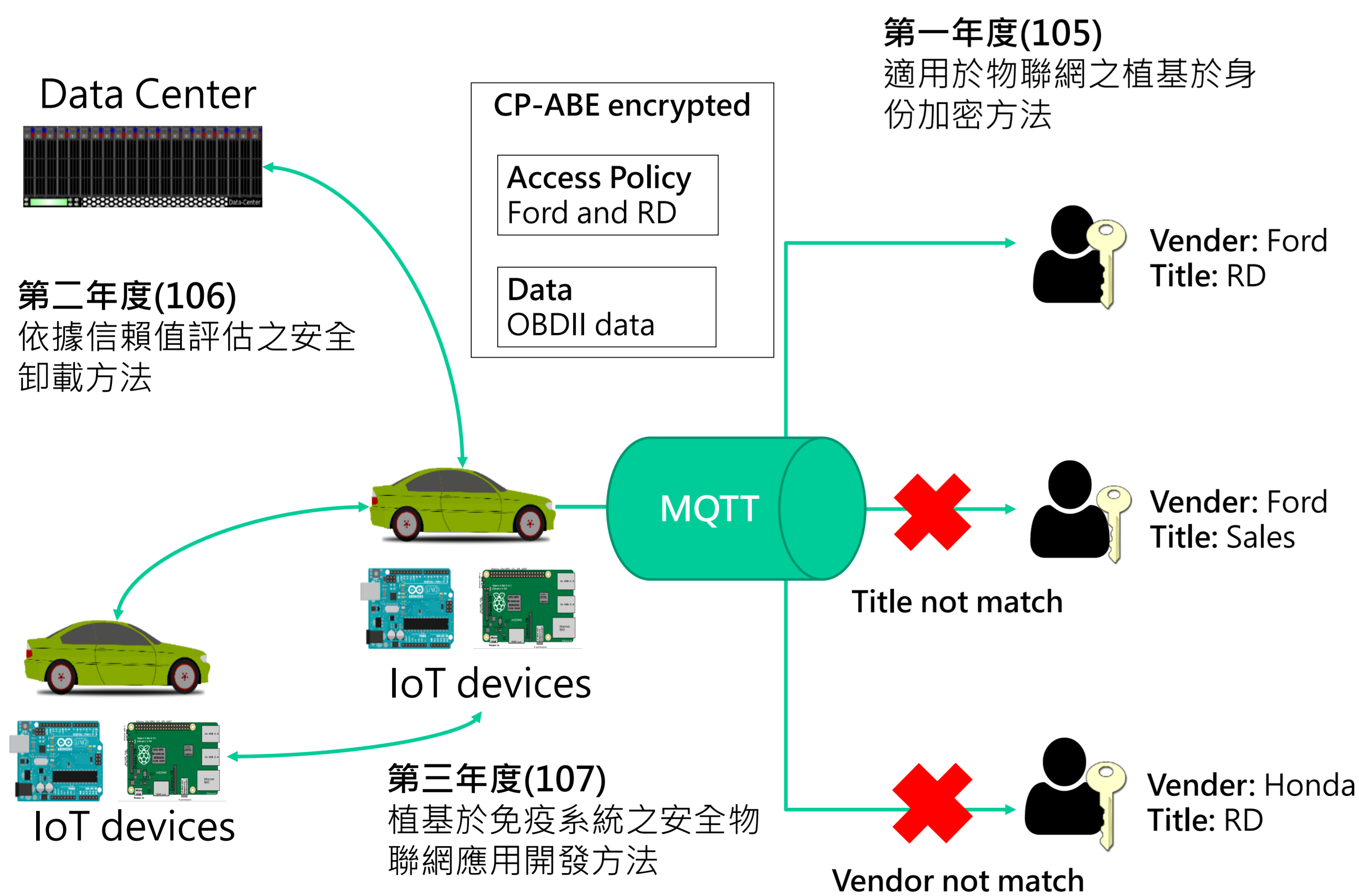
本子計畫「植基於免疫系統之安全的物聯網應用開發方法 - 以先進駕駛輔助系統為例」的目標即是在確保由大量車輛上先進駕駛輔助系統(ADAS)所產生之感測資料透過網路傳送到雲端資料中心進行儲存與運算的過程當中資料的安全性。為了能夠有系統地完成研究目標，我們提出一個包含「適用於物聯網之植基於身份加密方法」、「植基於信賴值量化之加密卸載方法」以及「多階段裝置異常檢測之類免疫編程模型」等技術的三年期研究專案。首先，「適用於物聯網之植基於身份加密方法」的研究目標是讓物聯網裝置所產生的資料能夠在確保安全性與隱私權的條件下細緻地(fine-grained)給適當的使用者進行存取。此外，因為物聯網裝置的運算資源(例如、CPU 運算能力、記憶體大小等)有限且是透過電池供電的，所以「植基於信賴值量化之加密卸載方法」的研究目標是在物聯網裝置的運算資源無法支援複雜的加密運算時可以透過將複雜的安全性運算卸載(offloading)到鄰近可信賴的裝置來滿足其安全性需求。最後，「多階段裝置異常檢測之類免疫編程模型」的研究目標則是如何在物聯網應用的開發階段就以編程模型來加入安全性機制。透過植基於免疫系統之安全物聯網應用編程模型所開發的物聯網應用，可以在執行階段中透過產生資安檢查樣本(security-checking samples)以讓裝置本身、鄰近裝置、資料傳輸過程中的中間裝置、或設計者都可以藉由比對該裝置過去的行為來進行多層次的自我資安檢測。

#### 效益與特色

本計畫【植基於免疫系統之安全的物聯網應用開發方法】具有以下效益與特色：

- 設計與實作「適用於物聯網之植基於身份加密方法」在物聯網裝置數量急遽增加的環境中以確保資料安全性與隱私權為前提下提供細緻地(fine-grained)的存取控制。
- 設計與實作「依據信賴值評估之安全卸載方法」讓資源有限的物聯網裝置能將複雜的加密運算卸載(offloading)至鄰近裝置並利用統計模型分析裝置行為(包含如資源、安全、與正確性等參數)來量化信賴度以提高運算卸載的效益與安全性。
- 設計與實作「植基於免疫系統之安全物聯網應用開發方法」在物聯網應用的開發階段就以編程模型來加入安全性機制在執行階段中進行多層次的自我資安檢測

#### 使用情境圖



#### 技術應用範圍

- 可以物聯網服務供應商合作開發有安全需求的應用
- 提供物聯網應應用開發套件

#### 本年度(105)計畫成果

##### 開放原始碼：Project Bee

基於物聯網通訊協定(MQTT)之開放原始碼專案提供

- 點對點的安全性(MQTT原本只提供TLS)。
- 整合第一年計畫成果「適用於物聯網之植基於身份加密方法」以屬性加密方法(CP-ABE)提供細緻化的存取控制以符合物聯網的安全性與分享性需求。

<https://github.com/adas-most/adas-security-mqtt/tree/master/bee-cpabe-sdk-0.1>

##### 學術論文

- Wei-Tsung Su and Kuan-Yew Lee, "Design and Implementation of Three-tier Home Automation Architecture," 2017數位生活科技研討會
- Wei-Tsung Su and Chao-Yi Kao, "EstiTO: An Efficient Task Offloading Approach based on Node Capability Estimation in a Cloudlet," 2017 IEEE Wireless Communications and Networking Conference, Mar. 19-22, San Francisco, USA. (MOST 105-2221-E-156-004)
- Wei-Tsung Su and Cheng-Yi Dai, "QoS-Aware Distributed Cloud Storage Service based on Erasure Code in Multi-Cloud Environment," The 14th Annual IEEE Consumer Communications & Networking Conference (Work In Progress paper), Jan, 8-11, 2017, Las Vegas, USA. (MOST 105-2221-E-156-004)