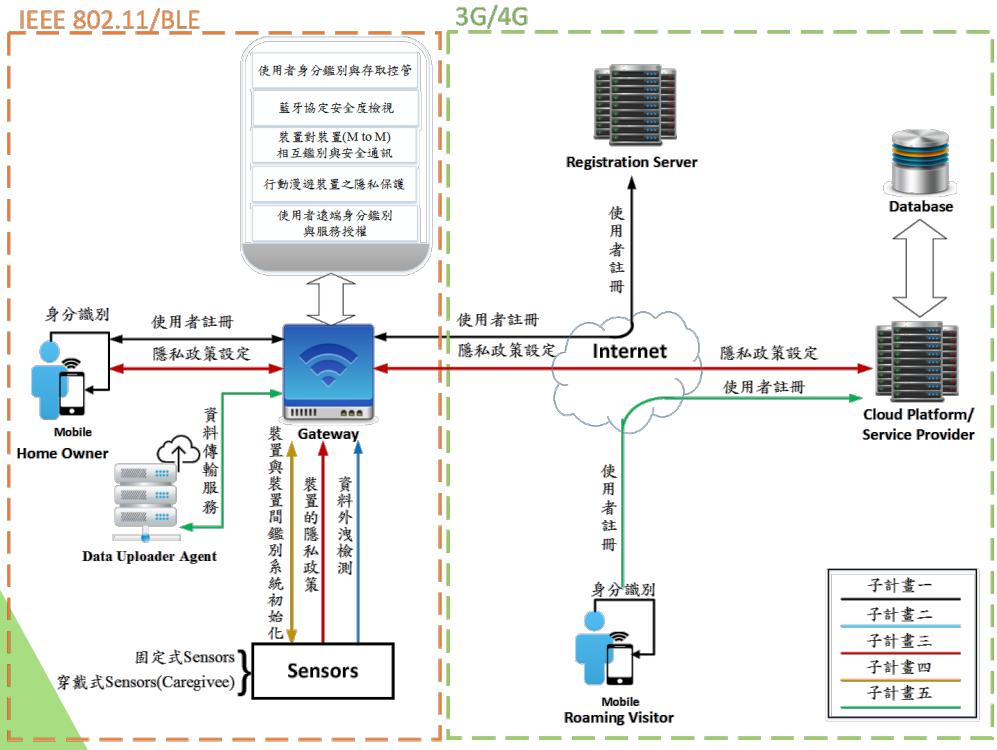
總計畫名稱：IoT可信賴架構之設計與實作
執行單位：臺灣科技大學/資訊管理系
主持人：吳宗成 教授
計畫編號：MOST 105-2221-E-011-070-MY3

一、摘要
本計畫設計並開發IoT可信賴架構(IoT Trusted Architecture)，完成物聯網裝置之使用者身分鑑別與存取控管、藍牙協定安全度檢視、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模組。並以智慧家庭為例，驗證該IoT可信賴架構之實務可行性。

二、架構功能
IoT可信賴架構在智慧家庭應用之參與角色包含家庭成員/訪客(Home Owner/Roaming Visitors)、感測器(Sensor)、閘道器(Gateway)、雲端平台(Cloud Platform)，並滿足以下安全功能需求：

- 家庭成員/訪客：執行使用者註冊/身分鑑別、提供使用者查詢鄰近感測裝置之資訊與隱私政策。
- 感測器：支援與閘道器間相互鑑別及傳送裝置的隱私政策。
- 閘道器：接收及記錄感測裝置資料、鑑別使用者身分並落實資料存取控管。
- 雲端平台：定期接收閘道器傳送之資料，提供使用者遠端存取功能。



三、技術特色
- 建立兼顧本地及遠端存取之輕量化使用者身分鑑別與存取控制機制。
- 運用自動化藍牙封包擷取與分析元件，檢視藍牙協定之傳輸安全性。
- 建立隱私協商機制，協助使用者掌控自身資料。
- 適用於物聯網環境之裝置對裝置安全通訊協定。
- 運用鑑別式金鑰協議(AKA)，發展適用4G網路下之身分鑑別機制。

四、技術應用範圍
- 提供各式物聯網環境下之使用者的身分鑑別、隱私保護、遠端存取控管。
- 支援物聯網裝置之隱私風險評估，以有效掌控機敏資訊外洩風險。
- 支援自動化感測裝置與閘道器之相互鑑別需求，建立可信任的通訊管道。

總計畫名稱： IoT可信賴架構之設計與實作
子計畫名稱：使用者物聯網裝置啟動之使用者鑑別協定與控管機制

執行單位：臺灣科技大學/資訊管理系
主持人：吳宗成 教授

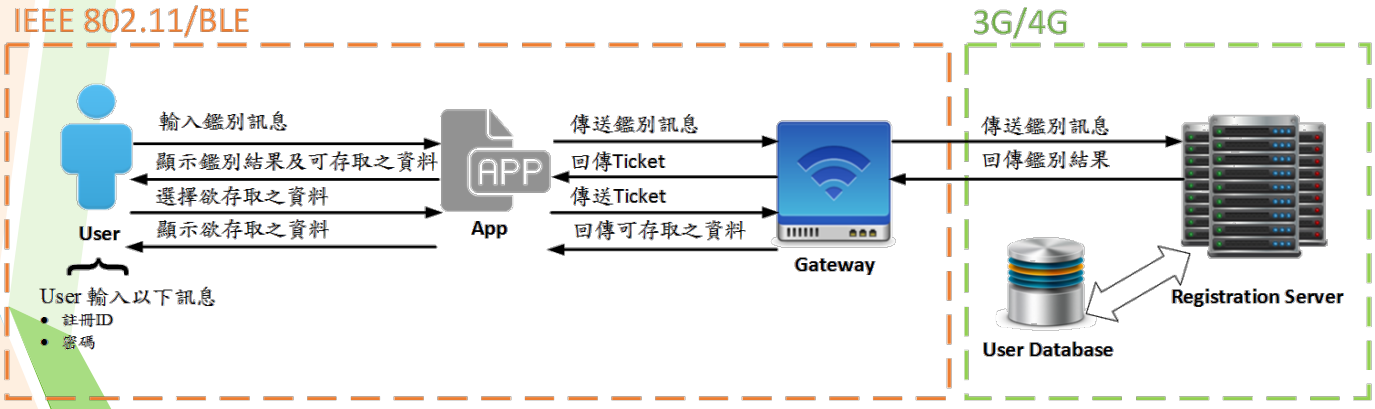
計畫編號： MOST 105-2221-E-011-070-MY3

一、摘要

傳統的使用者鑑別協定與存取控管機制，大多採用基於高計算複雜的密碼學理論，未能適用於具資源限制之物聯網環境。本計畫發展輕量化使用者身分鑑別與存取控制機制，可支援智慧家庭環境下之本地使用者與閘道器之間的身分識別及資料存取控管。

二、架構功能

使用者鑑別協定與存取控制機制的主要參與角色包含使用者(User)、閘道器(Gateway)及註冊伺服器(Registration Server)。透過手持裝置的App應用程式，使用者傳送鑑別訊息給閘道器，並轉送給註冊伺服器進行身分鑑別及授權資料比對。比對成功後，閘道器產出授權的Ticket並回傳給手持裝置的App應用程式。隨後，使用者可透過該App應用程式暫存的Ticket向閘道器提出資料存取授權請求。



三、技術特色

- 在既有之IEEE 802.11/BLE及3G/4G標準協定下，建立兼顧本地及遠端存取之輕量化使用者身分鑑別與存取控制機制。
- 利用Ticket的時效性，可有效控管存取權限。

四、技術應用範圍

- 依據不同的資料授權策略，強化使用者身分鑑別及資料存取權限控管。
- 在可信賴的IoT環境下，可對不同使用者採取相對應的資料存取設定。