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

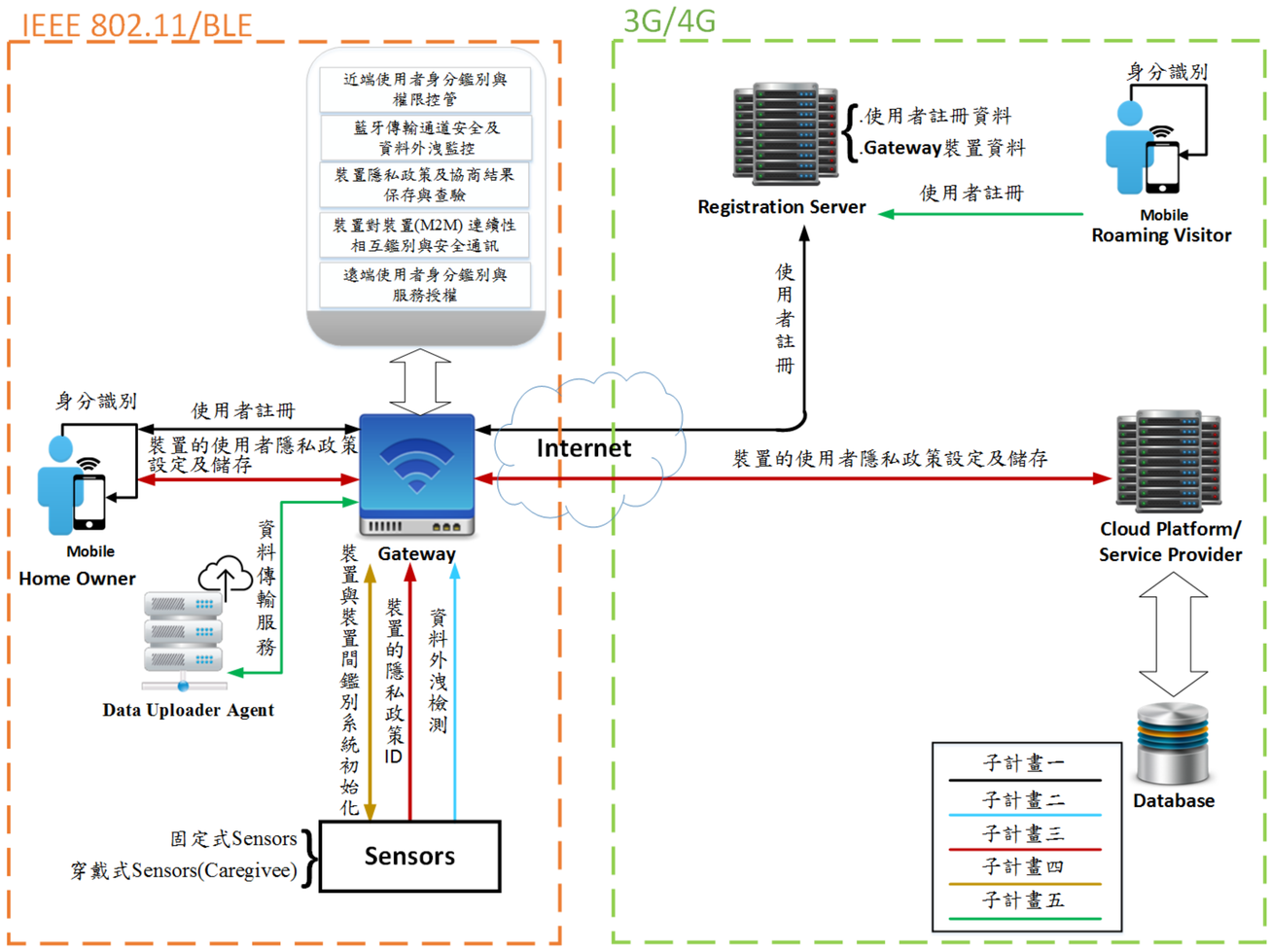
一、摘要

本計畫設計並開發IoT可信賴架構(IoT Trusted Architecture)，完成物聯網裝置之近端使用者身分鑑別與權限控管、藍牙傳輸通道安全及資料外洩監控、裝置隱私政策及協商結果保存與查驗、裝置對裝置(M2M)連續性相互鑑別與安全通訊、遠端使用者身分鑑別與服務授權等功能模組。並以智慧家庭為例，驗證本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)，所使用的裝置包含手持行動裝置(Mobile Device) 、感測器(Sensors)、閘道器(Gateway)、註冊伺服器(Registration Server)、雲端平台(Cloud Platform)，並滿足以下安全功能需求：

- ■ 手持行動裝置App：提供使用者註冊/身分鑑別/設定角色權限功能、搜尋鄰近感測裝置功能與查詢各感測裝置之使用者隱私政策功能。
- ■ 感測器：支援與閘道器間連續性相互鑑別及提供使用者之隱私政策偏好。
- ■ 閘道器：接收及記錄感測裝置資料、鑑別使用者身分並提供資料存取控管。
- ■ 註冊伺服器：記錄使用者註冊資料、使用者閘道器相對應之角色及權限資料。
- ■ 雲端平台：定期接收閘道器傳送之資料，提供使用者遠端查詢及存取功能。



三、技術特色

- 建立兼顧近端及遠端存取之輕量化使用者身分鑑別與權限控管機制。
- 開發自動化藍牙封包擷取與分析元件，以檢視行動裝置藍牙連線之資料傳輸安全性。
- 運用區塊鏈技術儲存感測裝置資訊、使用者隱私政策與協商結果，防止資料被不當讀取或竄改。
- 運用互斥或函數、雜湊函數、雜湊訊息鑑別碼實作輕量化裝置對裝置連續性身分鑑別協定，可抵擋各種主要攻擊手段，並支援資料完整性、相互鑑別與前向安全性之特性，以確保感測裝置與閘道器間之連線安全。
- 發展適用於4G網路環境之裝置鑑別機制，以建立閘道器與雲端平台間的安全通訊。

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、權限控管、隱私保護、遠端存取控管。
- 揭露使用者在物聯網環境下進行隱私風險，有效掌控使用者機敏資訊外洩之情況。
- 支援感測裝置與閘道器之自動化連續性相互鑑別，建立安全的通訊管道。

臺灣科大

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

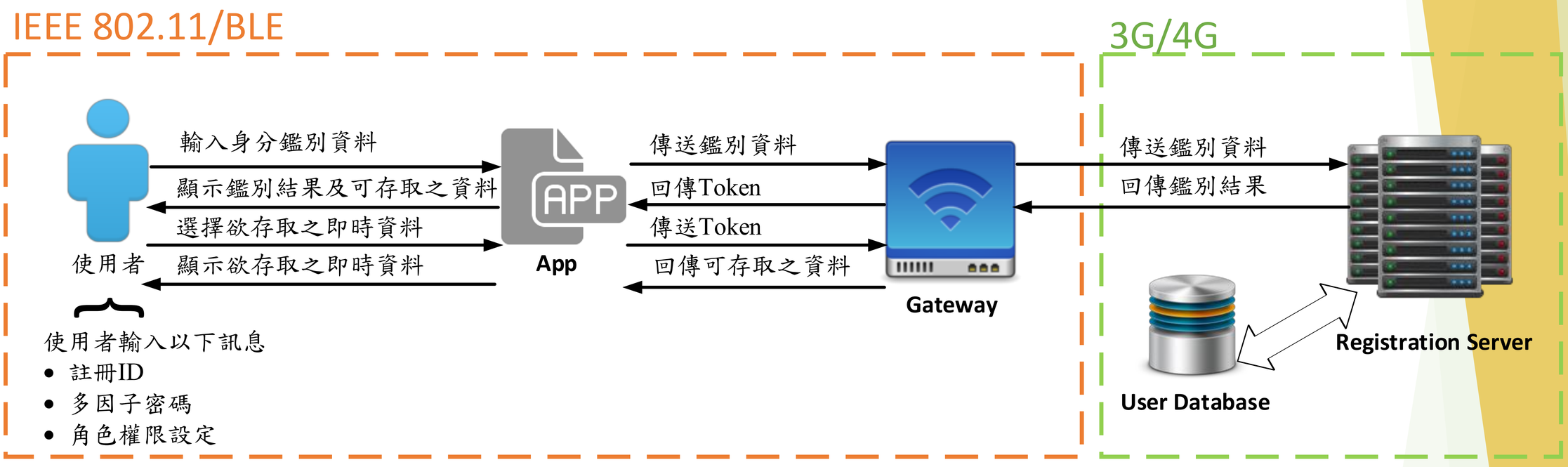
計畫編號： MOST 105-2221-E-011-070-MY3

一、摘要

傳統的使用者鑑別協定與資料存取機制，大多採用計算複雜的密碼系統，未能適用於充斥大量計算資源匱乏的感測裝置之物聯網環境。本計畫發展輕量化使用者身分鑑別與權限控管機制，透過令牌(Token)確認使用者之身分與裝置合法性，並以角色存取權限管理資料存取與授權時間。

二、架構功能

使用者身分鑑別協定與權限控管機制的主要角色包含使用者(User)所持有之行動裝置、閘道器(Gateway)及註冊伺服器(Registration Server)。使用者透過手持行動裝置的App應用程式，經由閘道器(Gateway)向註冊伺服器進行身分鑑別，以取得相對應權限之令牌，使用者可運用該令牌向閘道器取得資料。



三、技術特色

- 在既有之IEEE 802.11/BLE及3G/4G標準協定下，建立兼顧近端及遠端存取之輕量化使用者身分鑑別與權限控管機制。
- 結合多因子鑑別(Multi-factor Authentication)技術，可提升本協定身分鑑別之強度。

四、技術應用範圍

- 運用角色授權機制，企業可簡化使用者權限控管程序，營造使用者友善的環境。
- 在可信賴的物聯網環境下，使用者可方便進行近端及遠端伺服器的身分鑑別及資料存取。