總計畫名稱：IoT可信賴架構之設計與實作
子計畫名稱：物聯網裝置與家庭閘道器之感測層鑑別與安全通訊技術

執行單位：臺灣科技大學/資訊管理系
主持人：羅乃維 教授

計畫編號： MOST 105-2221-E-011-080-MY3

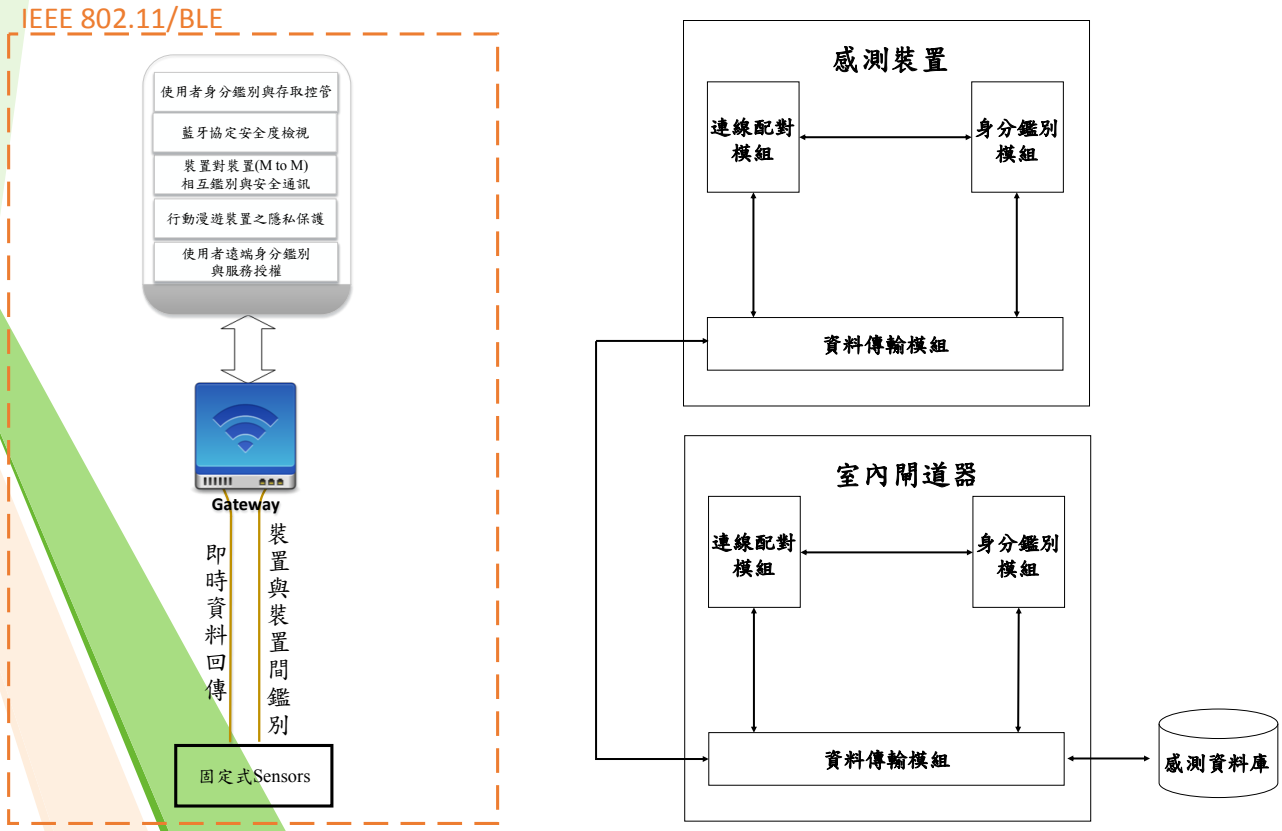
一、摘要

物聯網在應用上，會依需求佈建許多不同功能的感測裝置及一個以上的閘道器，而雙方在傳遞資料時，需要確認彼此的身分及保持資料的完整性；然而感測裝置本身的運算資源通常有限，無法負擔傳統鑑別協定的繁雜運算，所以本計畫的目標是設計並實作適用於感測裝置與閘道器之間自動化、輕量化裝置對裝置身分鑑別協定以建立可信任的通訊管道。

二、架構功能

本計畫設計感測裝置與閘道器之身分鑑別協定，可檢驗資料在進行傳輸的過程中是否遭受他人竄改，以確認資料完整性；亦可檢驗資料是否來自合法的裝置，以確認資料來源真實性。本協定的實作由下列三個模組構成：

- **連線配對模組**：建立感測裝置與閘道器之間的連線配對。
- **身分鑑別模組**：確認感測裝置與閘道器雙方的身分合法性。
- **資料傳輸模組**：確保完整資料可於感測裝置與閘道器間正常傳送與接收。



三、技術特色

- 運用雜湊、互斥或、雜湊訊息鑑別碼等運算方式來實作輕量化裝置對裝置身分鑑別協定，可支援運算資源較缺乏的物聯網感測裝置。
- 可抵擋重送攻擊、假冒攻擊、中間人攻擊，提高整體物聯網環境安全性與可信任性。

四、技術應用範圍

- 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。