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：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

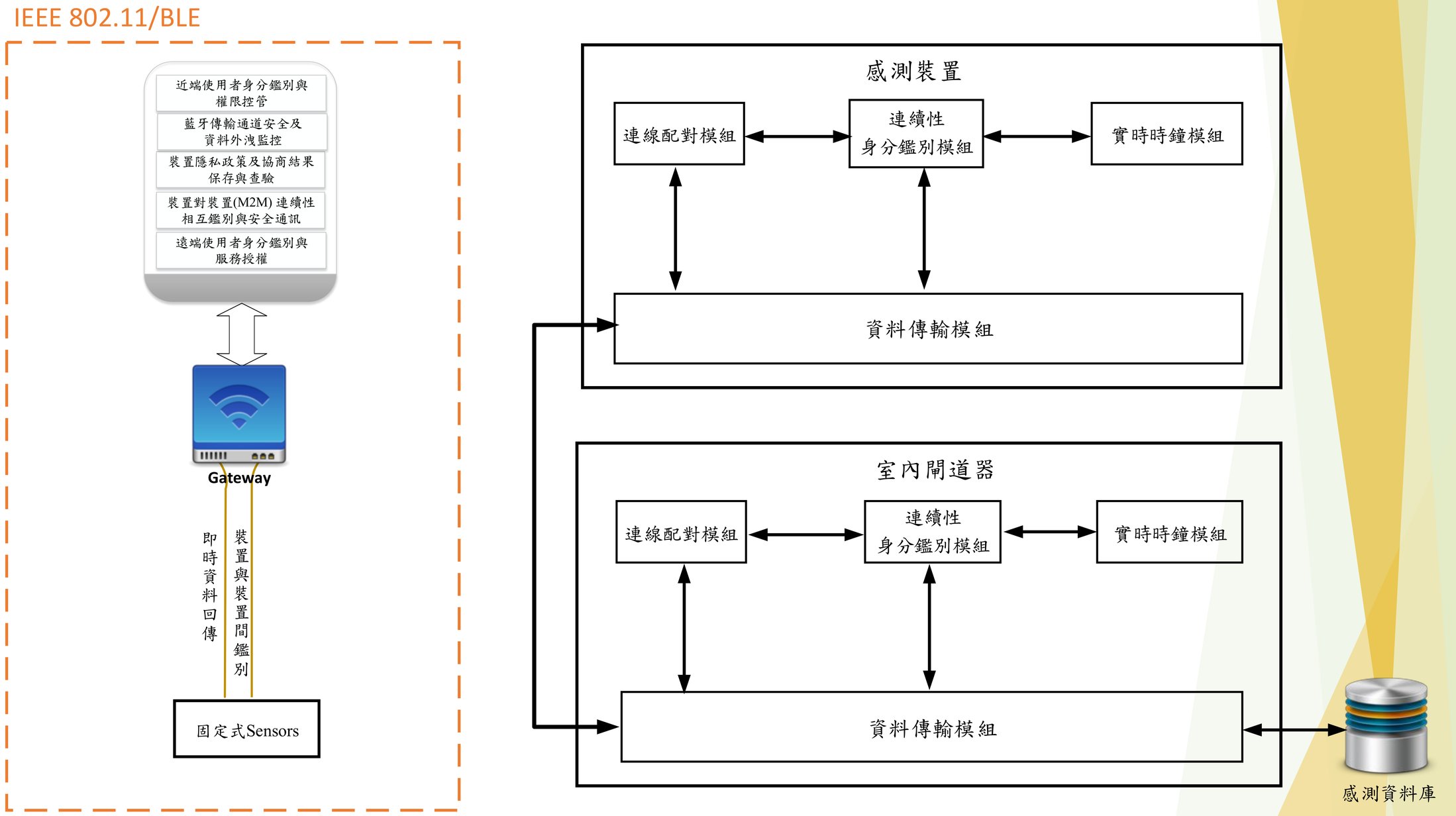
一、摘要

物聯網在環境應用上，會依需求佈建許多不同功能的感測裝置及一個以上的室內閘道器(Interior Gateway)，而雙方在傳遞資料前，需要快速鑑別感測裝置與室內閘道器相互間的身分並建立安全通訊管道；然而感測裝置通常只擁有有限的計算資源，因此無法負荷傳統鑑別協定的繁雜運算。本計畫目標是設計並實作針對室內環境的感測裝置與室內閘道器之間的輕量化連續性身分鑑別協定與安全通訊機制。

二、架構功能

本計畫設計感測裝置與閘道器之連續性身分鑑別協定，此協定可保持資料完整性並確認資料來源。本協定的系統實作由下列四個模組構成：

- 連線配對模組：建立感測裝置與閘道器之間的連線配對。
- 連續性身分鑑別模組：確認感測裝置與閘道器雙方的身分合法性及傳輸資料完整性。
- 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。
- 實時時鐘模組：負責提供連續性身分鑑別模組存取實時時鐘之數值。



三、技術特色

- 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，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。

四、技術應用範圍

- 支援感測裝置與閘道器之自動化連續性相互鑑別需求，並建立安全的通訊管道。