總計畫名稱：IoT可信賴架構之設計與實作
子計畫名稱：物聯網架構下適用於家庭雲環境之身分即服務機制

執行單位：政治大學/資訊科學系
主持人：左瑞麟 副教授

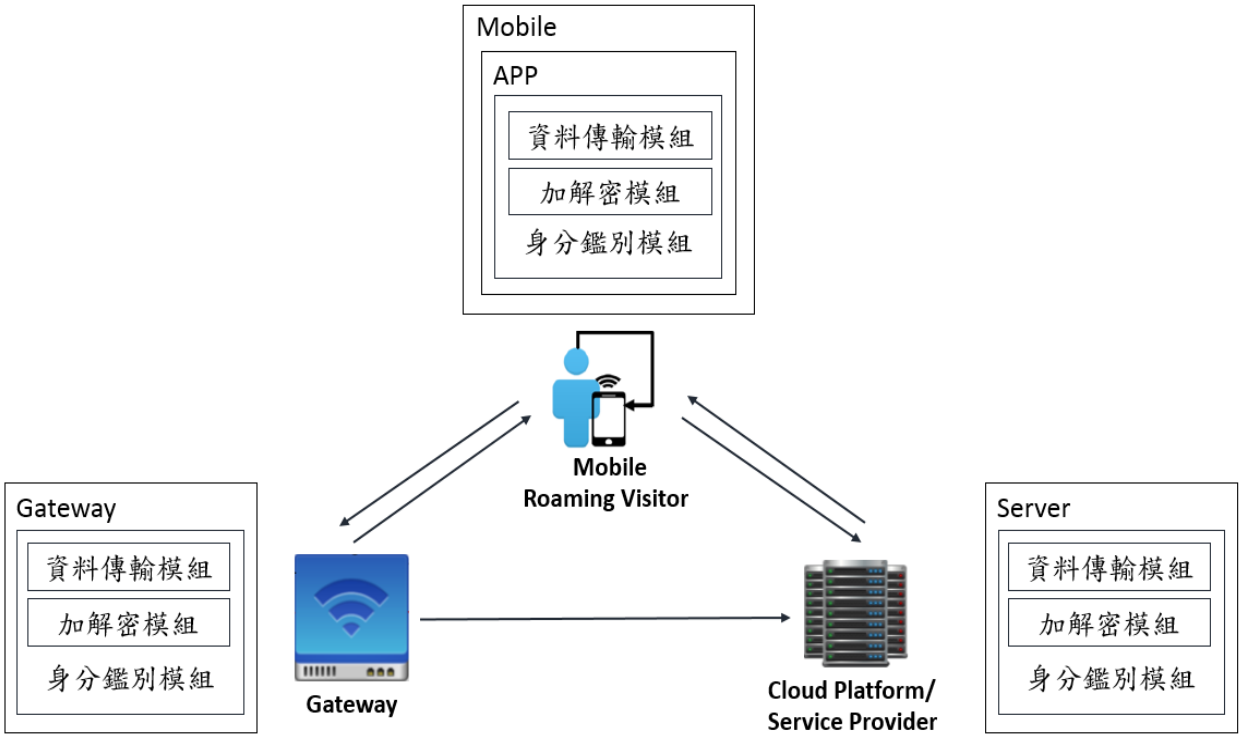
計畫編號： MOST 105-2221-E-004-001-MY3

一、摘要

本計畫主要在探討物聯網之網路層中，用戶遠端登入及4G網路下資料傳輸時所需面對之安全議題。研究目的在設計適用於4G網路環境中之輕量級身份鑑別機制、金鑰協議與資料完整性驗證模組設計。

二、架構功能

物聯網架構下適用於家庭雲環境之身分即服務機制可讓室外使用者(Roaming Visitor)安全的使用及查看家中感測器裝置資料，利用本計畫所設計可應用於4G網路之輕量化身分鑑別機制，透過簡單的帳號密碼登入App，取得存取閘道器(Gateway)或伺服器的Token，爾後即可透過Token取得資料。若欲取得即時資料則向閘道器(Gateway)發出存取需求；若欲取得歷史資料則向伺服器(Server)發出存取需求，將結果顯示給使用者。



三、技術特色

- 結合SHA3-512及XOR運算方法，降低運算複雜度，達成系統輕量化之目的。
- 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

- 協助行動裝置使用者在4G網路下有效防護其機敏資訊，並降低隱私外洩風險。
- 協助行動裝置使用者在4G網路下，與智慧家庭閘道器及伺服器進行身分鑑別。