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

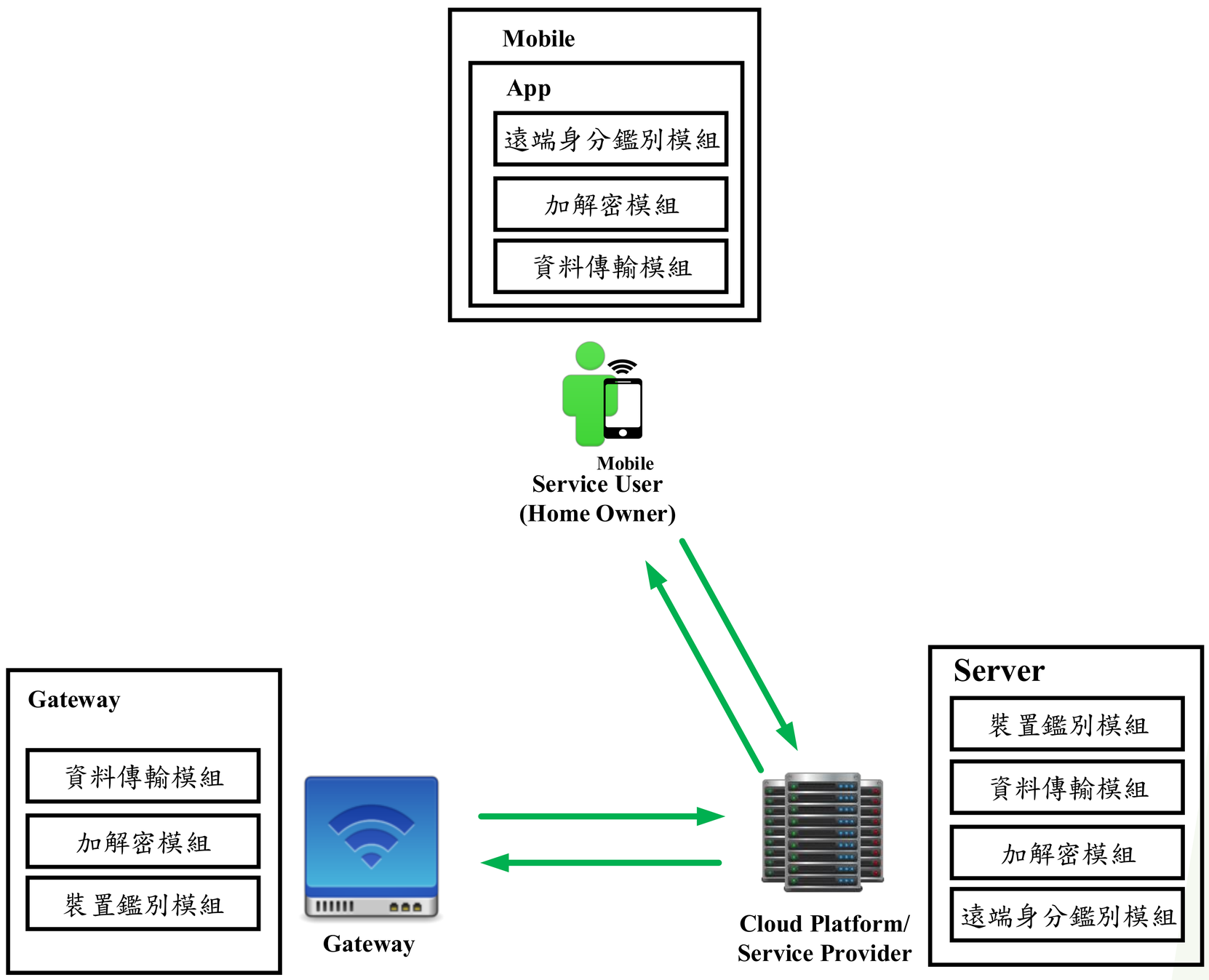
計畫編號： MOST 105-2221-E-004-001-MY3

一、摘要

本計畫主要探討物聯網中，使用者透過4G網路進行遠端用戶登入及進行機敏資料傳輸時所面對的安全議題。具體研究包含4G網路環境之身分鑑別機制以及基於Diffie-Hellman密鑰交換的安全通訊機制之設計。本計畫發展出使用者可利用輕量級身分鑑別機制遠端登入智慧家庭環境存取資料，並透過密鑰交換機制建立閘道器與雲端平台間的安全通道，以確保使用者的隱私安全及資料傳輸的機密性。

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家庭使用者(User)在遠端亦能透過持行動裝置App經由4G網路連線至家庭雲環境，並存取家中感測器裝置所儲存的歷史資料或即時資料。當開啟手持行動裝置App進行遠端連線時，雲端平台透過基於雜湊函數之身份鑑別協定確認使用者身份後，發送令牌(Token)給使用者。使用者即可透過令牌取得資料。若欲取得即時資料則透過伺服器(Server)向閘道器(Gateway)發出存取需求；若欲取得歷史資料則向伺服器發出存取需求，將結果顯示給使用者。



三、技術特色

- 發展基於雜湊函數的身份鑑別協定，達成認證系統輕量化之目的。
- 利用Diffie-Hellman密鑰交換協定，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

- 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，與智慧家庭閘伺服器進行遠端身分鑑別。