以ESP32實現之BLE KEYLESS LOCK

專題成員:高司玹 指導教授:李皇辰

摘要

現代人生活節奏快，人們常常身上攜帶著多種物品，例如手機、錢包、購物袋等等。在這樣的情況下，需要尋找鑰匙或處理現金交易可能會導致不必要的延誤和不便。

而付錢或是近距離開門的自動化由於都是近距離的動作，即當在主人在周圍時，裝置才可以做相對應的動作，因此就須仰賴無線測距的功能來協助完成，因此我想要借用BLE無線測距功能來實現。

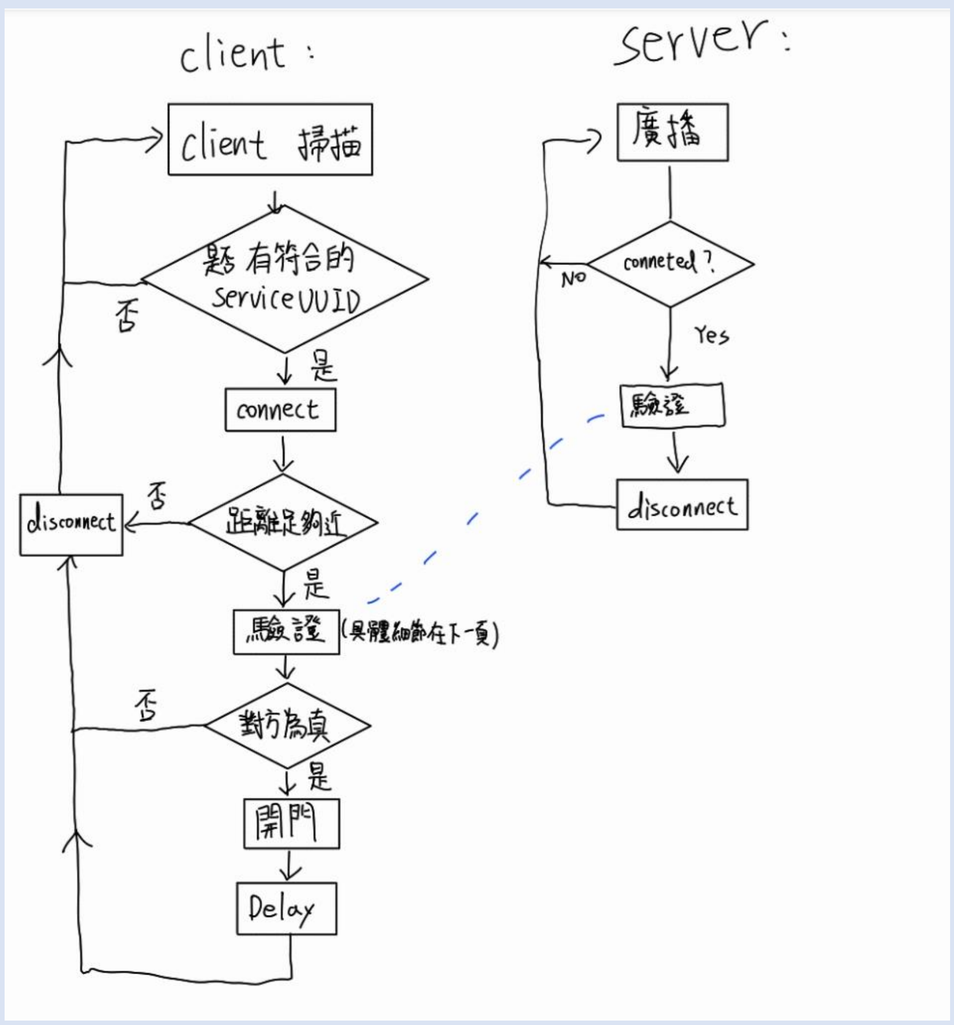
此外付款或開門的自動化不僅僅是關於便利性，還關係到個人隱私和財務安全。因此，本研究除了要結合BLE無線測距技術實現近距離操作，同時還要包括身份驗證機制，確保只有授權用戶能夠執行這些操作。

在本專題中，我們將以Keyless門鎖作為目標示例，採用ESP32作為實現的平台。不僅要實現無線測距功能，還要設計一個安全的驗證系統，以確保只有合法的使用者可以啟動門鎖。

設計方法:

■ 兩塊esp32，一個做為門鎖(client)，另一個做為鑰匙(server)，彼此以BLE溝通。

■ 當鑰匙靠近門鎖一定距離後，會驗證鑰匙的身分，若正確則開門。



圖(一)

Client端不斷掃描，Server是不斷廣播，當雙方的UUID是對的便會連接(connect)，連接後便會檢查彼此距離，必須距離接近一定數值時才會後才會進入下一步，如圖(一)

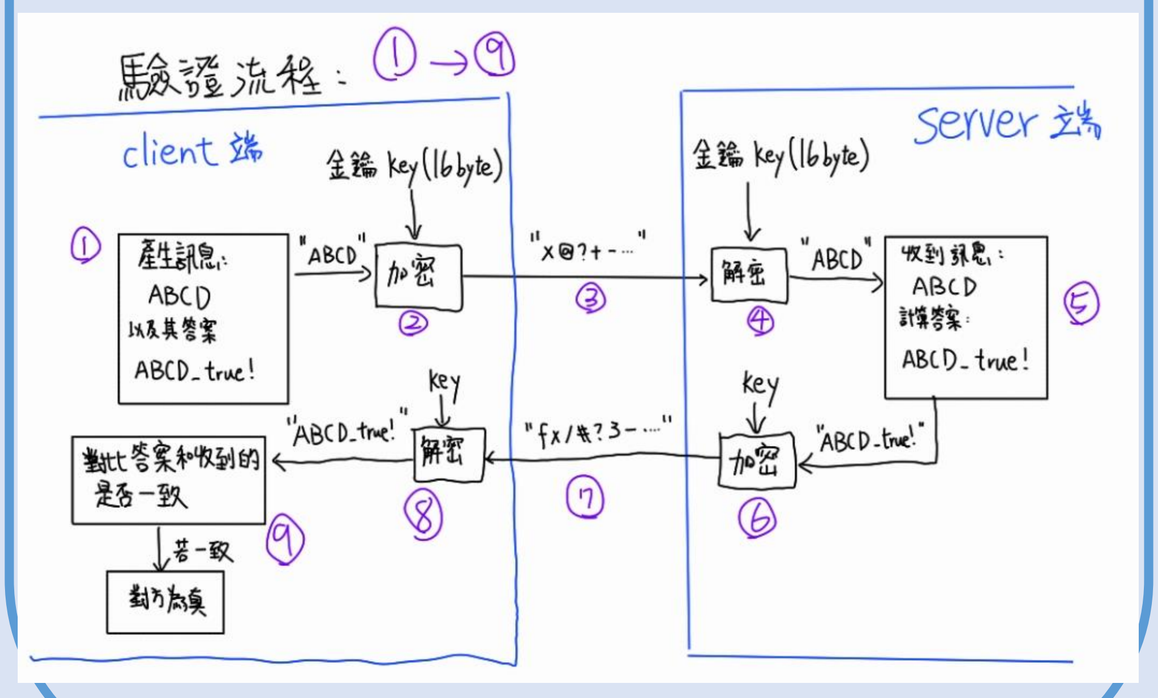
驗證方法如下:

雙方透過對稱式加密AES溝通，雙方擁有同一筆金鑰(16byte)(事先寫好在雙方程式內，因此除非記憶體洩漏等因素，不然只有溝通的雙方知道)

client隨機產生一段訊息(<=16byte)並加密傳給server，serve收到後便根據訊息產生一段對應的答案，唯有當server能夠正確解密這段訊息才能產生正確的答案，因此client只要確認對方的回覆的答案是否正確，就能證明對方是不是假冒的。

而此時會有個問題，若每次的訊息都是一樣的，則每次傳回的答案都會是固定的，那麼入侵者將可以模仿(流程7)中帶的加密的答案通過，即便入侵者看不懂這串加密文字的涵義。

因此為了避免此情況，client端每次產生的訊息是隨機的，所以每次的答案也不會固定。

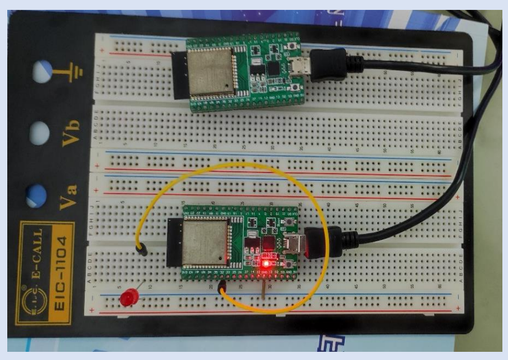


圖(二)

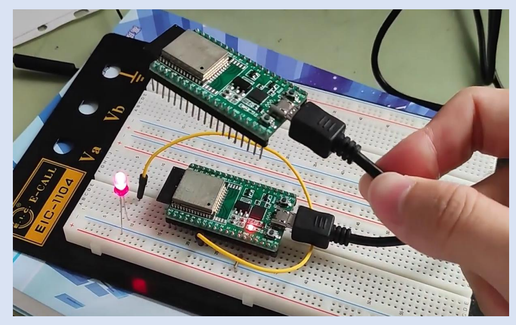
成果展示:

這邊以紅色LED亮來表示解鎖。

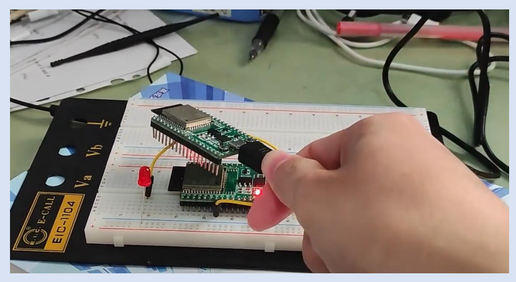
上方為鑰匙，下方為門鎖。



Case 1: 正確密碼且距離足夠接近設定的值。



Case 2: 如果是錯誤的密碼，即便距離夠近也不會解鎖。



Case 3: 正確密碼但距離過遠。不解鎖