

社群媒體與對話機器人系統設計

期末專案成果報告

GPU 購物小幫手

資訊安全

專案成員

資工四 107590012 陳志榮

資工四 107590037 應耀德

目錄

社群媒體與對話機器人系統設計 期末專案成果報告 GPU 購物小幫手 資訊安全 專案成員 資工四 107590012 陳志榮 資工四 107590037 應耀德	1
一、專案主題	3
二、Website	4
2.1 會員整合流程設計	4
2.2 認證授權	5
2.3 使用者登入認證、內容授權	6
2.4 整合測試、結果截圖	6
三、Report	9
3.1 統計報表內容	9
3.2 使用者登入認證、內容授權	10
3.3 整合測試、結果截圖	10
四、期末專案心得	11

一、專案主題

本專案設計一套電商購物推播系統，讓顧客(Customer)能夠追蹤指定商品，進行下訂單的動作，並且在商家補貨後，會第一時間收到 Line bot 推播的補貨通知，讓顧客不錯過購買時機，同時也能查看市場統計報表，查詢商品的熱賣程度，以及品牌熱門度。管理員(Administrator)可以管理商品、管理訂單，並且能查看統計報表，並查看商品的銷售報表、營業額報表。

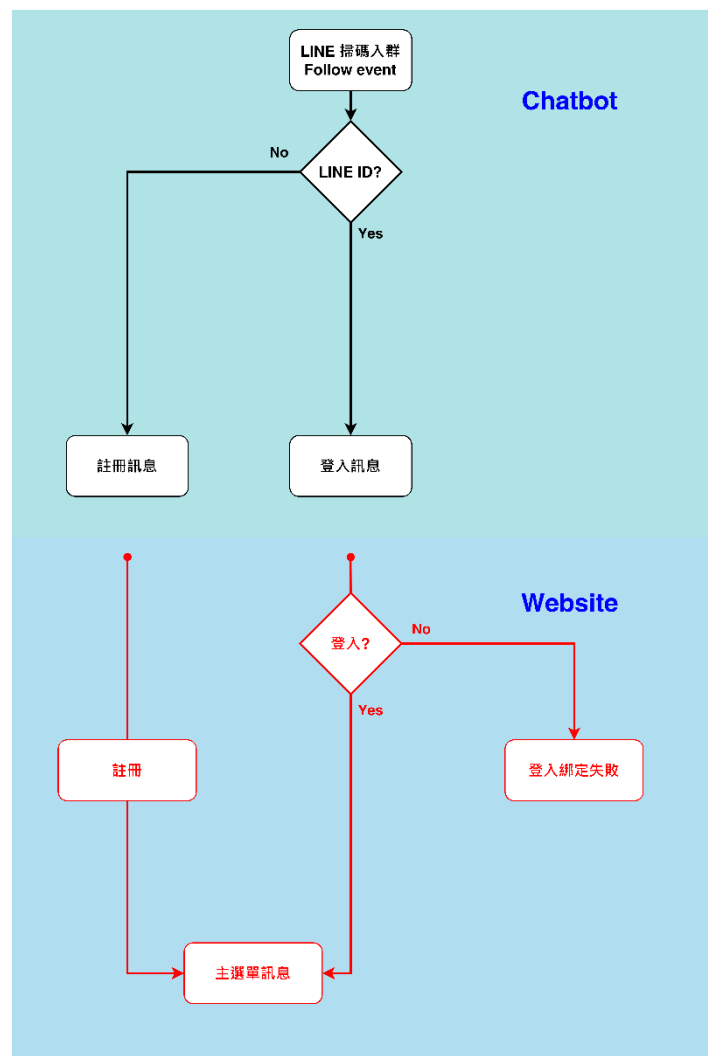
本專案以 GPU 庫存的追蹤購買為例子，未來可擴充成不同商品類型的 Line bot，亦可以經營成電商平台的形式，定期的推播新貨通知以及優惠商品。

此次成果報告進行資訊安全的設計，對使用者在網站上的操作行為進行安全性的控管，對應使用者角色給予應有的功能權限以及報表存取權限，以達到資訊安全的目的。

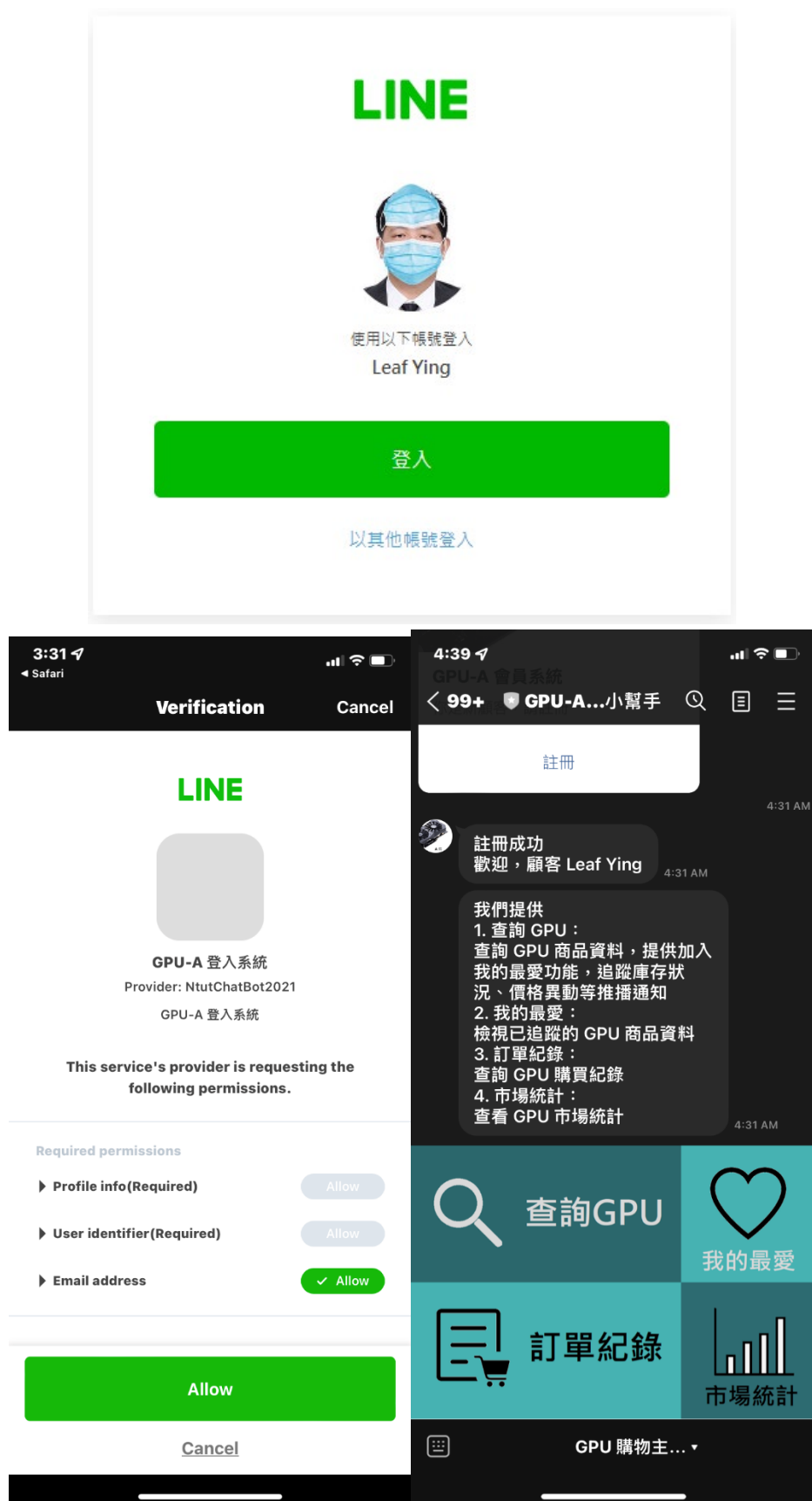
二、Website

2.1 會員整合流程設計

	 LINE A	 LINE B
會員註冊	未註冊	已註冊
Chatbot	註冊訊息	登入訊息
Website	登入/註冊	登入
	主選單訊息	主選單訊息




2.2 認證授權



2.3 使用者登入認證、內容授權

功能 \ 角色	anonymous	customer	seller	admin	權限
登入	○	○	○	○	
註冊	○	○	○	○	
會員綁定	×	○	×	×	@jwt_required、@roles_required
查詢GPU	×	○	○	×	@jwt_required、@roles_accepted
管理商品	×	×	○	×	@jwt_required、@roles_required
我的最愛	×	○	○	×	
查詢訂單	×	○	○	×	@jwt_required、@roles_accepted
管理訂單	×	×	○	×	@jwt_required、@roles_required

2.4 整合測試、結果截圖

	 LINE A	 LINE B
前置作業		Web 登入/註冊 掃碼入群 封鎖退群
狀態	未註冊	已註冊
登入註冊	掃碼入群 註冊訊息 登入/註冊 主選單訊息	解除封鎖 登入訊息 登入 主選單訊息

測試前

	id	username	email	line_id	role_id
1	74516529ebb6143503637e64e4ac5be1	Leaf Ying	yqhua@gmail.com	Ud5ccb684684e312e0626f522fc8af34f	1

測試後

	id	username	email	line_id	role_id
1	4dc472661582950aacd24943651bdbd0	Ron	yoyotv5290@yahoo.com.tw	U8aafe21ac37194f9a889f3a7f2993f13	1
2	74516529ebb6143503637e64e4ac5be1	Leaf Ying	yqhua@gmail.com	Ud5ccb684684e312e0626f522fc8af34f	1

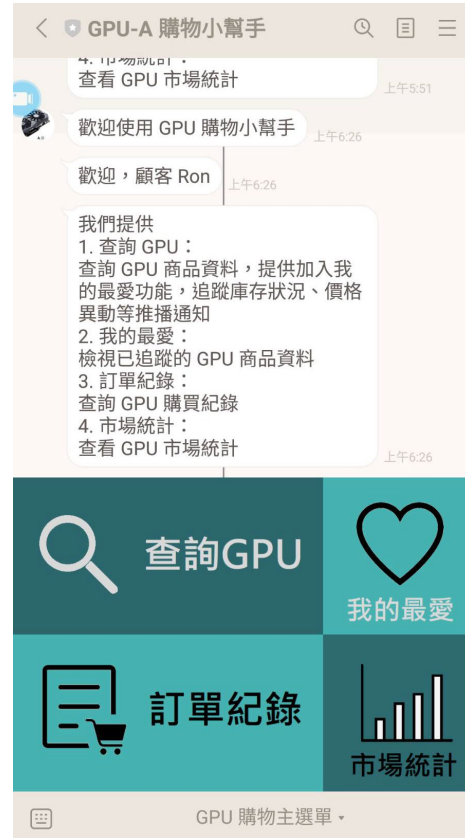
LINE A 未註冊

顯示註冊 menu



LINE B 已註冊

註冊成功訊息並顯示 richmenu



封鎖後解除封鎖顯示登入 menu



API Gateway 測試

With x-api-key

New Collection1225 / New Request

GET

https://gputest-ja3xvj4.an.gateway.dev/company/TinkQBepEnT080eEICe

Send

Params

Authorization

Headers (6)

Body

Pre-request Script

Tests

Settings

Headers

5 hidden

KEY	VALUE	DESCRIPTION		Bulk Edit	Presets
<input checked="" type="checkbox"/> x-api-key	AlzaSyAkQ2sGMrpLfwW4EQ_r2xCWKrEypH9BEMg				
Key	Value	Description			

Body

Cookies

Headers (14)

Test Results

Pretty

Raw

Preview

Visualize

JSON

1

2

3

4

5

6

200

200

200

200

200

200

{}
"response": {
 "id": "TinkQBepEnT080eEICe",
 "name": "GPU-AI"
}

Status: 200 OK

Time: 3.56 s

Size: 854 B

Save Response

Without x-api-key

FinalAPIGatewayTest / New Request

GET

https://apigatewayserver-2-ja3xvj4.an.gateway.dev/company/ vER7zvAXi2B3kzIBK90Q

Send

Params

Authorization

Headers (6)

Body

Pre-request Script

Tests

Settings

Headers

5 hidden

KEY	VALUE	DESCRIPTION		Bulk Edit	Pre
<input type="checkbox"/> x-api-key	AlzaSyAkQ2sGMrpLfwW4EQ_r2xCWKrEypH9BEMg				
Key	Value	Description			

Body

Cookies

Headers (6)

Test Results

Pretty

Raw

Preview

Visualize

JSON

1

2

3

4

200

200

200

200

{}
"message": "UNAUTHENTICATED:Method doesn't allow unregistered callers (callers without established identity). Please use API Key or other form of API consumer identity to call this API.",
"code": 401

Status: 401 Unauthorized

Time: 391 ms

Size: 577 B

Save Response

三、Report

3.1 統計報表內容

市場統計：For anonymous, customer



統計報表：For seller, admin



3.2 使用者登入認證、內容授權

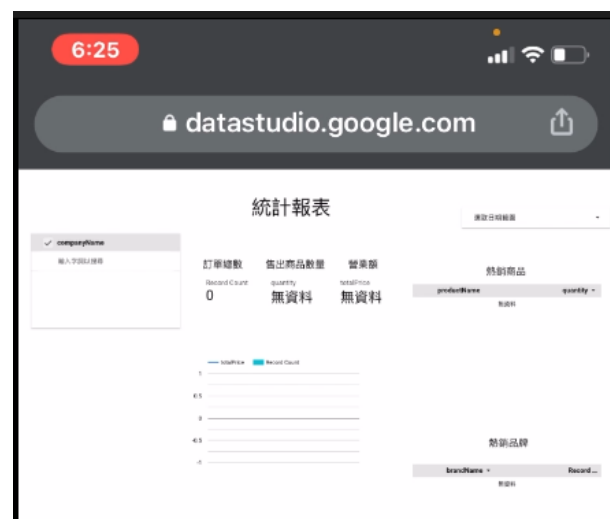
功能 \ 角色	anonymous	customer	seller	admin	權 限
市場統計	○	○	×	×	@jwt_required(optional=True)
統計報表	×	×	○	○	@jwt_required、@roles_accepted

3.3 整合測試、結果截圖

Customer 點擊 richmenu 市場統計



Seller、Admin 點擊 richmenu 統計報表



四、期末專案心得

應耀德：

這次負責 Website 與 Line bot webhook 安全驗證流程設計與實作，學到如何串接 LINE LOGIN，達到 SSO 登入，也為了瞭解 OAuth 授權驗證流程，花了時間在閱讀 standard sheet，如何驗證 CSRF Token、如何防止 Replay attack 等，也設計一套 redirection 流程，能夠記住登入前的網站，登入之後能夠重新導回前一頁。

除此之外，此次使用的 security library 並不是作業所使用的 Flask-Security-Too 而是使用 Flask-JWT-extended 套件，但該套件沒有支援 role-based 授權功能，所以按照官方的文件造了一個 @role_accepted decorator，同時也嵌入 remember_page=True/False 的 redirection 機制，也就是於第一段所介紹 rediectection 流程。

這門課程對我來說是第一門雲端課程，使用到許多服務，學習資源非常多，也非常扎實。教授所設計的作業幫助我踏入雲端系統應用與設計，了解不同服務間如何串接、安全性權限如何設定、密鑰管理員如何使用等等。自己有先前的網頁後端系統建置與設計的經驗，在這門課也幫助我很多，照著 GCP 文件上實際操作後，自己能夠推敲出背後運作方式，這點對我來說非常重要，也謝謝教授開了這門課，讓我在大四畢業前充分理解雲端服務應用。

陳志榮：

這次負責的是 Api Gateway 和 data studio security 的部分，由於購物機器人的功能較多，需要規劃的 API 有很多，因此 yaml 檔只有實作一部份功能，而 data studio 的安全性規劃部分，因為在 Linebot 的 richmenu 部分已經先對不同的 role 採取前端分離，因此報表的部分也是相對地導向不同的 data studio report url，我認為這是一個更加安全的形式，因為作業中的 manger 和 admin 可以藉由 url 的 parameter 去存取對應的報表網址，只要藉由更改網址參數即可獲取別家商店甚至全部商店的報表，我認為存在著很大的資安漏洞，因此前端分流搭配導向不同的 report url 會是更安全的做法。

感謝老師的教學、助教的範本，以及最最最厲害的組員，因為我本身前後端的 coding 能力不足，因此整學期專案都是在挫折中學習，之前大三資料庫在本地端架設就弄得焦頭爛額了，而這門課的專案甚至要架設在雲端上，許多工具交錯使用，達成多樣性的功能，縱使吸收整體架構，在摸索上仍然四處碰壁，因為自己的不足而拖累組員，真的感到十分抱歉，我的能力尚無法達到如此高的程度，我會繼續努力精進自己。