

# HW10

任務:使用 Python 或 Weka 建立 SVM、RandomForest、CNN 模型,判斷 Android App 是否為惡意軟體 (二元分類)-(更新:二元分類、多類別分類都可)

資料集:CICMalDroid2020

---

## 1. 從原始 APK 取特徵

- 請說明取特徵的方式
- 無法成功取特徵的 apk 可略過,但須註明每類的失敗數量

## 2. 前處理 (資料輸入進模型前的所有步驟)

## 3. 建立 SVM、RandomForest 及 CNN 模型

(至少包含以下內容)

- 說明資料如何訓練/測試 (e.g. Hold-out, Cross Validate, etc. )
- 超參數調整
- 說明模型架構及參數設定(有附原因佳)
- 註:CNN 不可使用現有架構

## 4. 【加分題】使用現有 CNN 架構訓練,並與自行建立的 CNN 做比較

## 5. 評估報告

(至少包含以下內容)

- 分析結果,須有表格或圖統整同一模型不同超參數表現、各模型表現
- 使用的方法的優點或缺點
- 是否有可改進之處
- 最後會選擇哪一個模型(可自行假設情境)

**\*\* 門檻：** 未達門檻會扣一點點分數

- SVM (Acc: 0.93)

- RandomForest 、 CNN (ACC: 0.95 )

- 
- 繳交期限：6/26(六) 23:59，檔名為 ECT\_HW10\_學號
  - 請繳交答案卷(.pdf)和 python 程式檔(若有)，pdf 檔請註明題號。若使用 weka 請將過程與輸出截圖證明；若使用 python 請將重要程式片段截圖。

上傳至 ee-class 作業區，遲交一天扣該次作業 5%