**附件 四、模型效能量測說明文件格式**

**「類神經正切泛化攻擊模型」(模型名稱)**

**模型訓練說明文件**

**建置團隊：子計畫二**

**子計畫名稱：可信賴AI之資料處理與模型理論\_\_\_\_\_\_\_\_**

**子計畫主持人：\_\_\_\_吳尚鴻\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**說明文件版本：v1**

**日期：2022/8/13**

1. **模型效能量測說明**

| **模型中文名稱** | 類神經正切泛化攻擊模型 |
| --- | --- |
| **模型英文名稱** | Neural Tangent Generalization Attack |
| **模型編號** | M201 |
| **效能量測所使用之資料集名稱** | MNIST |
| **效能量測所使用之資料集來源** | <http://yann.lecun.com/exdb/mnist/> |
| **效能量測所使用之資料集取得方式** | 網路下載 |
| **效能量測所使用之資料集取得/上架時間** | 1998年 |
| **效能量測所使用之資料集檔案大小** | 2MB |
| **效能量測所使用之資料集檔案類型** | Testing set : 10000張圖片每張圖片為28 \* 28的黑白圖片 |
| **效能量測所使用之資料集是否包含個資與隱私，資料授權方式** | 否 |
| **效能量測所使用之資料之標記資料來源與類型** | 資料來源：<http://yann.lecun.com/exdb/mnist/>類型如：pixel-wise |
| ** 模型使用之GPU或CPU使用資源** | 2021/07 |
| **模型使用之記憶體使用量** | GPU : V100 |
| **模型之使用空間** | 32G |
| **模型預期之測試執行時間** | 42MB |
| **模型預期之測試結果輸出類型** | image |
| **模型預期之測試結果類型** | 此模型為生成圖片使模型無法成功學習，依照模型的種類結果會不同。 |
| **模型預期之測試結果** |  |

備註：效能量測所使用之資料集應與訓練以及驗證所使用之資料集不同