FaceIDoor – 智慧門鎖

NM LAB Final Project

B09901106 莊加旭 B08901014 謝承霖 B08901168 翁茂齊

Introduction

電機系為台大最大系，不論學生數量或系館數量皆為台大之首。如此龐大的學生量與系空間使得辨認學生身份變得困難。

現今門禁政策為使用學生證之RFID刷卡，擁有該卡片者即可暢通無阻，使得眾多昂貴器材暴露在被偷竊、破壞的風險下。

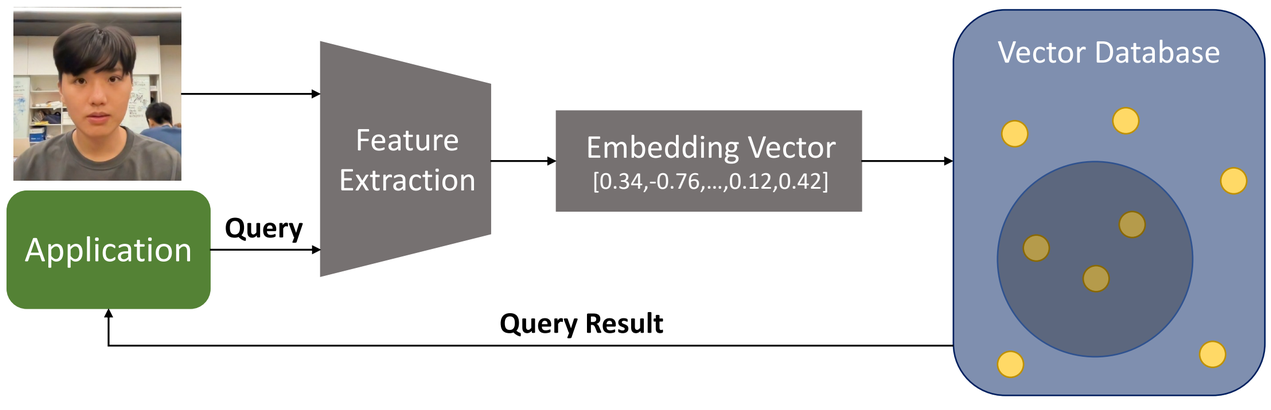
我們做出與 FaceID 相同功能的FaceIDoor，將RPi基於 TPM (what you have) 與 AI 臉部辨認 (who you are) 的元素建出類 FIDO2 的無密碼登入流程，使得系館存放重要器材地區不會被簡單進入。

Work Flow

使用者註冊時，我們會掃描他的臉部特徵當作 SRK password ，在使用者的 TPM 上升成一組新的公私鑰，並將公鑰儲存在伺服器的資料庫中。

登入時，我們會再次要求使用者掃描臉部資訊提供給 TPM ，並且發送一個挑戰請 TPM 簽署。最後，我們的伺服器會用註冊時儲存在資料庫中的公鑰來驗證這個簽章，完成登入流程。

Biometric Authenticator



Feature Extraction

- Model Architecture: InceptionResnetV2
- Embedding Vector: 512 dim
- Face Detection -> Image Crop -> Feature Extraction

Vector Database

- Query vector based on similarity metric
- Approximate Nearest Neighbor (ANN) search
  - Hashing, Quantization, Graph-based search
- Features
  - Data management, Scalability, Real-time updates

Technique

- tpm2-tss engine
- tpm2-tools
- Pinecone
- DeepFace
- Flask
- OpenCV
- OpenSSL
- Next.js
- trpc
- redis

Flow Chart