Private Mobile Chatbot Application

김동훈, 이윤상, 김민영

Goals & Problem

Main Goal: 안드로이드용 Heaan SDK를 적용하기 위한 NDK 제작 및 라이브러리화 진행 및 Heaan SDK를 활용한 챗지피티 기반 챗봇 서비스 제작

Problem

Heaan의 동형암호 라이브러리는 메모리가 많이 필요하기에 모바일에 적합하지만, 아직 안드로이드 라이브러리화는 진행되지 않은 상태. 앱으로 라이브러리화해도 Heean 쪽 구현 예제가 없다.

Requirements

"Accessibility" : Expand Cryptolab API to Android platform using JNI and NDK

"Interactivity" : Implement ChatGPT in a mobile application chatbot

Approach

암호화가 필요한 앱 서비스로 **Finance User Complaint report application**를 선정.

유저들이 개인정보가 포함된 Finance Complaint를 앱으로 작성하면 암호화되어 분류되고, 또 사측에서 해당 complaint를 확인하는 서비스를 기획.

Development

안드로이드 앱

Android Studio

Kotlin

동형암호 안드로이드 라이브러리

Android NDK

C++

서버 및 분류모델

django

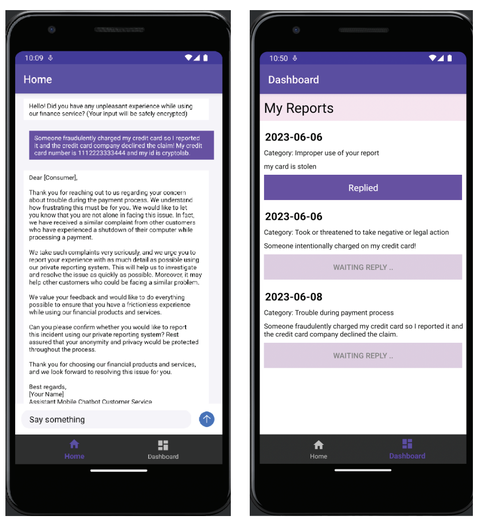
python

관리자 웹 서비스

NEXT.JS

Result

안드로이드 챗봇



사측 관리자용 웹 서비스

Future Work

- 현재로서 arm64-v8a만 지원하는 안드로이드 shared object file를 제작. 향후에 x86을 지원하는 안드로이드 shared object 제작이 필요

- 챗봇이 User Complaint만 받는 것으로 기능이 국한. 추후 발전을 위해 ChatGPT의 role 세분화 및 기능 추가

Implementation

1.안드로이드 라이브러리화

기존 Heean 라이브러리가 C++로 작성된 관계로. 필요한 코드를 ndk를 활용하여 arm용 shared_object 파일 (libHeaan.so) 컴파일 진행. 이 과정에서 C++ 라이브러리간 dependency 전체 resolve.

NDK

안드로이드 앱 쪽에서 C++ 함수를 호출할 수 있게 JNI로 C++ wrapper function 제작 및 인터페이스화.

2.모바일 client서 MPNet 임베딩 암호화

안드로이드에서 MPNet 토크나이저 나이브하게 구현 및 torch 기반 MPNet 모델을 tflite로 변환 후 후처리 진행.

임베딩에 필요한 encode_encrypt 함수를 안드로이드 단에서 전부 나이브하게 구현 (C++에는 encode_encrypt 함수가 없음)

3.암호화된 임베딩으로 서버에서 classification 수행

Client에서 넘긴 암호화된 임베딩 값을 받아들여서 암호화된 상태로 분류 모델이 작동하게끔 python Heaan SDK 적용.

python

4.서버에서 암호화된 분류 결과를 client에서 복호화

서버에서 결과값으로 도출하는 분류 또한 암호화되어있는 관계로 client 쪽에서 암호화된 임베딩을 보낼 때 서버에 저장되어 있는 유저의 public key와 함께 전달하는 프로세스 구현.

서버에서 분류 결과가 도착하면 secret key를 로드해서 분류 결과 복호화 후 사용자의 불만 카테고리 추출.

5.ChatGPT prompting

유저 단계별로 (총 6 stage) ChatGPT prompt 테스트 진행. ChatGPT의 role을 "kind helpful assistant"로 설정하고 user의 input을 바탕으로 챗봇 답변 생성.

6.챗봇 앱 개발

Kotlin

ChatGPT의 단계별 response에 대응하여 각 Step을 위한 step을 객체지향적인 방식으로 (Abstract Base Step Class 제작) 구현. 챗봇 및 열람 UI를 위한 ChatAdapter, RecyclerViewAdapter 제작.

7.관리자 웹페이지 서비스 개발

어드민이 사용자의 불만 리포트를 확인하고 답변할 수 있게끔 Histogram Chart UI 구현. Next.js로 제작하여 Vercel 에 Deploy.

NEXT.JS

HEAAN CRYPTO LAB