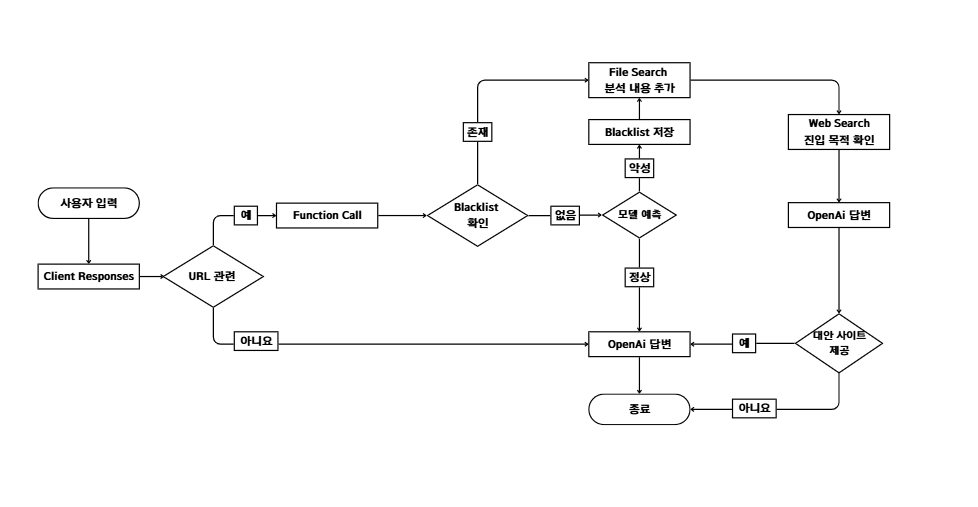
**PhishingGuard Chat 사용 설명서**

**1. 파일 구성**

| **파일명** | **역할 요약** |
| --- | --- |
| **Home.py** | Streamlit 기반 웹 인터페이스 |
| **agent.py** | 상위 에이전트 클래스 (대화 흐름 관리 및 Function Call 처리) |
| **main.py** | 단독 실행 가능 CLI 인터페이스 |
| **module.py** | URL 블랙리스트 검사 및 ML모델 예측 |
| **preprocess.py** | URL 전처리 기능 |
| **vector\_store.py** | OpenAI 벡터스토어 및 파일 업로드 기능 |
| **XGBoost\_model.pkl** | XGBoost 모델 훈련 및 평가 |

**2. 설계 구조**



**3. 사용 툴**

| **툴** | **역할 요약** |
| --- | --- |
| **websearch\_preview** | 사용자와의 일반적인 대화나 악성 url로 인한 대안사이트를 찾는 websearch |
| **file\_search** | 하위 에이전트에게 악성 url에 대한 전문적인 지식을 주기위한 file\_search |
| **function\_call** | 악성 url 관련 질문을 받았을 때 사용할 function\_call |

**4. 호출 함수**

**agent\_call :** 메인 에이전트가 악성 URL 관련 질문을 받았을 때 호출하는 함수입니다.

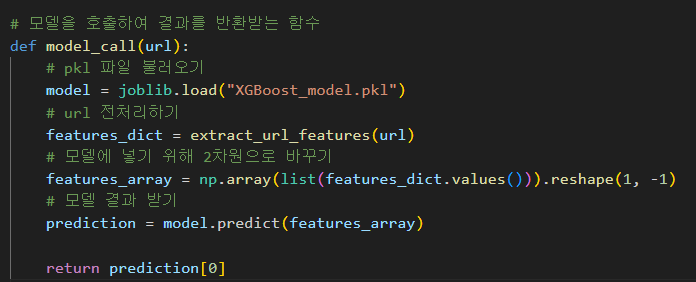
해당 호출 함수는 블랙리스트 검사 및 하위 에이전트 호출을 담당합니다.

**5. 모델 학습/사용법**

XGBoost 모델을 사용하며, 모델 학습 방법은 다음과 같습니다.

1. URL 컬럼이 있는 csv 데이터 셋을 준비한다.
2. [XGBoost.py](http://xgboost.py)에서 파일 경로를 해당 csv 데이터 셋으로 바꾼다.
3. XGBoost.py를 실행한다.
4. .pkl 파일이 저장된다.

이후, 모델 사용 예시 코드는 다음과 같습니다.



**6. 에이전트 상호작용**

┌───────────────────────────────┐

메인 에이전트

(사용자 질문 수신 및 제어)

└─────────────────┬─────────────┘

│

▼

사용자 질문: "이 URL이 안전한가요?"

│

▼

┌───────────────────────────────┐

Function Call 호출

(URL 정보 전달 및 작업 위임)

└─────────────────┬────────────┘

│

▼

┌───────────────────────────────┐

블랙리스트 및 모델 검사 모듈

(blacklist.csv + ML 모델 판단)

└─────────────────┬─────────────┘

│

▼

검사 결과: "악성" 또는 "정상"

│

▼

┌──────────────────────────────┐

하위 에이전트

(위 결과 기반 리포트 생성)

└─────────────────┬────────────┘

│

▼

리포트 전달

│

▼

┌───────────────────────────────┐

메인 에이전트

(최종 응답 생성 및 사용7자 응답)

└─────────────────┬────────────┘

│

▼

사용자에게 결과 응답

**7. 사용자 가이드**

1. <https://github.com/minhyung-aram/black_list_team_project.git>, git clone하기
2. requirements.txt를 사용하여 종속 라이브러리 다운로드
3. 따로 준비한 데이터 셋이 있을 경우 (5)의 내용을 토대로 학습하고 저장하기
4. [module.py](http://module.py)의 model\_call 함수에서 .pkl 파일 경로 설정
5. 커맨드라인에 **streamlit run** [**Home.py**](http://home.py)를 하여 streamlit 웹 실행

**8. 예시 시나리오 및 응답**



