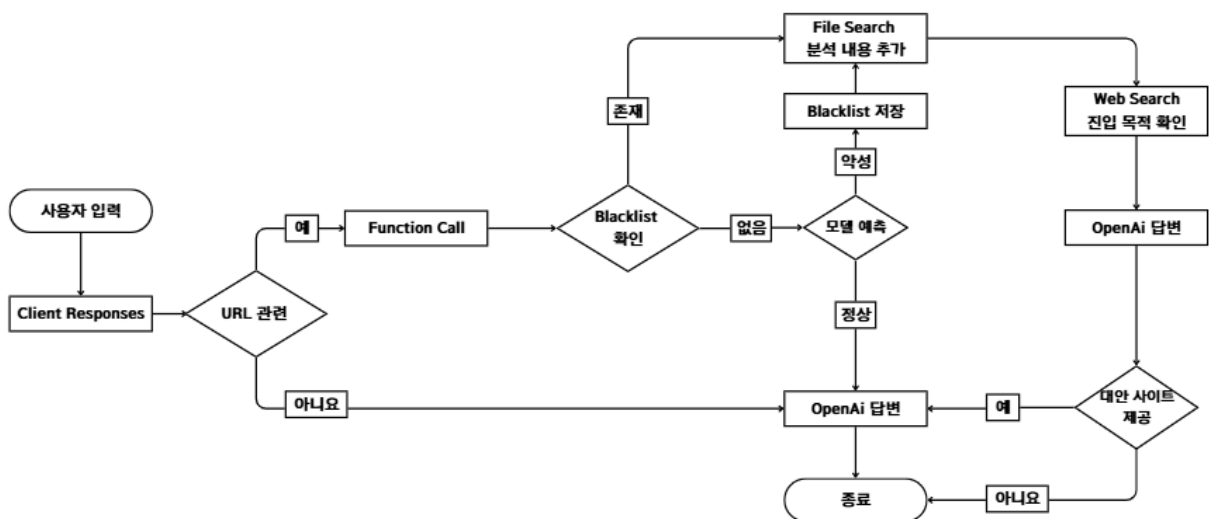


PhishingGuard Chat 사용 설명서

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.

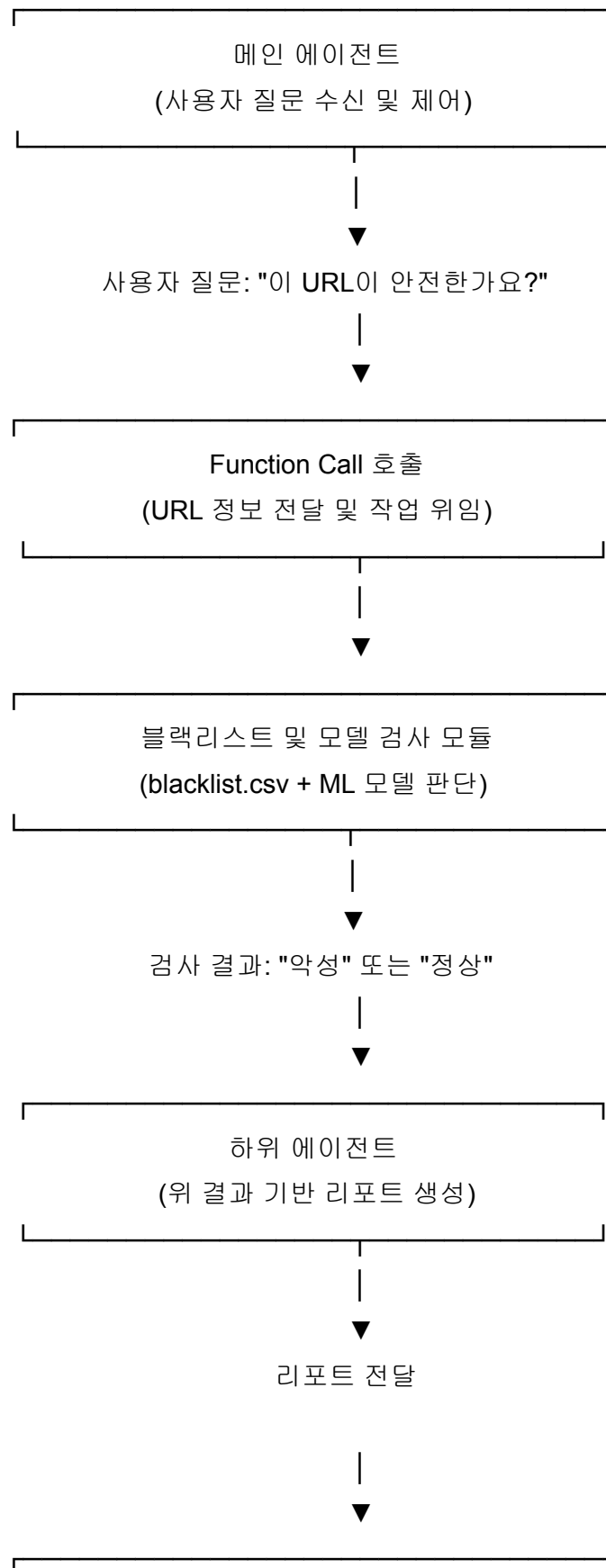
1. URL 컬럼이 있는 csv 데이터 셋을 준비한다.
2. [XGBoost.py](#)에서 파일 경로를 해당 csv 데이터 셋으로 바꾼다.
3. XGBoost.py를 실행한다.
4. .pkl 파일이 저장된다.

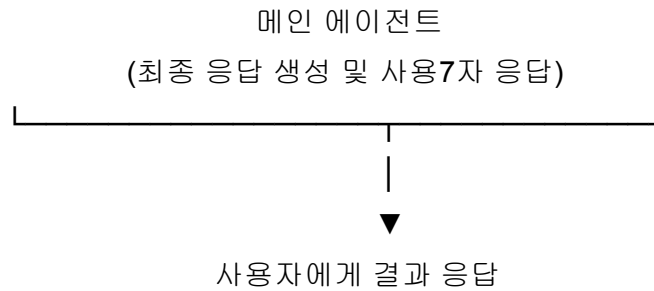
이후, 모델 사용 예시 코드는 다음과 같습니다.

```
# 모델을 호출하여 결과를 반환받는 함수
def model_call(url):
    # pkl 파일 불러오기
    model = joblib.load("XGBoost_model.pkl")
    # url 전처리하기
    features_dict = extract_url_features(url)
    # 모델에 넣기 위해 2차원으로 바꾸기
    features_array = np.array(list(features_dict.values())).reshape(1, -1)
    # 모델 결과 받기
    prediction = model.predict(features_array)

    return prediction[0]
```

6. 에이전트 상호작용







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](#)의 model_call 함수에서 .pkl 파일 경로 설정
5. 커맨드라인에 **streamlit run Home.py**를 하여 streamlit 웹 실행


8. 예시 시나리오 및 응답

 <http://oir.g7ut.yachts> 이거 정상 url이야?

 해당 URL(<http://oir.g7ut.yachts>)은 블랙리스트에 등록된 악성 URL로 확인되었습니다. 이 사이트를 방문하지 않는 것이 좋습니다.

사용 목적에 맞는 대안 사이트를 추천해드릴까요? 목적을 알려주시면, 안전한 사이트를 찾아드리겠습니다.

 <http://yn.k1mn.yachts> 이건?

 해당 URL(<http://yn.k1mn.yachts>)은 악성으로 판단되었습니다. 피싱, 멀웨어 배포, 데이터 절도와 같은 위험이 있을 수 있으니 방문하지 않는 것이 좋습니다.

혹시 방문하려는 목적이 무엇인지 알려주시면, 안전한 대안 사이트를 찾아드리겠습니다.



나 은행 예금하려고!



은행 예금을 위해 안전한 대안 사이트를 추천드리겠습니다. 다음은 신뢰할 수 있는 국내 은행의 공식 웹사이트입니다:

1. 국민은행: <https://www.kbstar.com>
2. 신한은행: <https://www.shinhan.com>
3. 우리은행: <https://www.wooribank.com>
4. 하나은행: <https://www.kebhana.com>

이러한 은행들은 공인인증서를 통해 안전한 온라인 뱅킹 서비스를 제공합니다. 공인인증서는 전자상거래 및 각종 온라인 서비스에서 사용자의 신원을 확인하고, 데이터의 무결성을 보장하는 전자적인 인증서입니다. (supportipz.com)

예금 상품을 비교하고 싶으시다면, 금융감독원에서 제공하는 '금융상품 한눈에' 서비스를 이용하실 수 있습니다. 이 서비스는 다양한 금융권의 예금 상품을 간편하게 비교할 수 있도록 도와줍니다. (etoday.co.kr)

안전한 금융 거래를 위해 항상 공식 웹사이트를 이용하시고, 공인인증서를 통해 본인 확인을 철저히 하시기 바랍니다.