

2025-2학기 LLM과 AI AGENT 개발 및 활용 FINAL PROJECT



집사부

부동산 상담 AI Agent 개발 프로젝트

DATE

2025. 12. 08

Table of Contents

집사부 AI Agent 프로젝트 발표 순서



01 프로젝트 개요 및 개발 배경

02 타겟 유저 및 기대효과

03 전체 시스템 아키텍처

04 RAG 구성 요소 및 파이프라인

05 집사부 6대 핵심 도구 (Tools)

06 기능 4. 복잡 질문 모드 - Planner 단계

07 기능 5. Tool 호출 루프

08 기능 6. LLM Judge 평가 시스템

09 사용자 장기기억 시스템

10 시연 및 Q&A

프로젝트 개요 및 개발 배경

복잡한 부동산 정보의 비대칭성을 해소하기 위한 AI Agent '집사부'



개발 배경 Challenges



복잡한 부동산 규제와 금융정책

6.27대책, 9.7대책 등 지속적으로 변경되는 정부 정책과 대출 규제, 세금 제도로 인해 일반인이 정확한 정보를 파악하기 어려움



기존 LLM의 한계

ChatGPT 등 범용 언어 모델은 한국 부동산의 특수성과 전문적인 최신 법령 정보를 깊이 있게 반영하지 못함



환각(Hallucination) 문제

최신 정책이나 특정 조건에 대한 세부 정보 부재로 인해 잘못된 정보를 생성하거나 검색 결과의 정확성이 떨어짐



개발 목표 Objectives



신뢰할 수 있는 정보 제공

공문서 기반의 명확한 출처와 근거 제시



합리적 의사결정 지원

객관적 데이터와 계산을 통한 의사결정 보조



정보 탐색 시간 단축

복잡한 정책을 일일이 찾지 않고 즉시 확인



부동산 정보 접근성 향상

정보 격차 해소 및 누구나 쉬운 접근

타겟 유저 | 기대효과



타겟 유저 PRIMARY AUDIENCE

부동산 거래를 계획하거나 현재 진행 중인 일반인

부동산 거래 경험이 전무한 대학생/사회초년생부터 경험을 보유한 일반인까지,
자주 변화하는 부동산 정책에 대해 정확하고 신뢰할 수 있는 정보가 필요한 모든 User

★ 핵심 기대효과



정보 탐색 시간 단축

복잡한 정책 문서를 일일이 찾아보거나
여러 출처를 비교할 필요 없이,

필요한 정보를 즉시 획득



정확한 정책 이해

명확한 근거 문서를 제시함으로써
정책 내용을 오해하거나

잘못 해석할 위험 최소화



합리적인 의사결정

대출 한도, DSR 계산 등 구체적 조건에
따른 맞춤형 정보를 제공하여

최적의 선택을 유도

전체 시스템 아키텍처

End-to-End 질문 처리 파이프라인 및 장기기억 저장 메커니즘



1. 질문 입력

User Query
사용자의 자연어 질문을
시스템에 입력



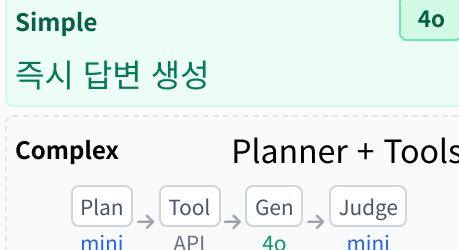
2. 난이도 분류

GPT-4o-mini
질문의 복잡도를 분석하여
최적의 경로 결정

Simple vs Complex



3. 실행 모드



4. 최종 답변

GPT-4o
답변 + 근거 문서 제공



참고문서.pdf



5. 장기기억

User Profile
사용자 취향/제약사항 저장
(다음 대화 시 반영)

Memory Updated

GPT-4o-mini

판단/계획 (비용 절감)

GPT-4o

생성/답변 (품질 우선)



Complex Process Chain

RAG 구성 및 검색 파이프라인

Upstage OCR과 FAISS를 활용한 고정밀 문서 처리 및 유연한 검색 전략



원천 문서

정책·법령 PDF
부동산 정책, 대출 약관
금융위원회 공문 수집



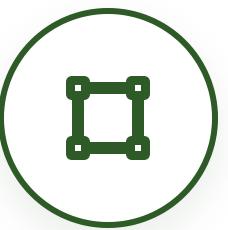
OCR 처리

Upstage API
고정밀 텍스트 추출
표/이미지 데이터 구조화



Chunking

최적화 분할
Token Size: 500
Overlap: 100



Embedding

Vector 변환
text-embedding-3-small
(OpenAI Model)



FAISS 검색

가변 검색 전략
기본 Top 3 조회
Planner 요청 시 확장

사용 도구 (Tools)

부동산 특화 답변을 위한 전문 도구 모음

search_vector_store

FAISS 기반 RAG 문서 검색으로 정확한 근거를 찾습니다.

- ✓ 참고 공문 [다운로드 링크](#) 자동 제공

search_korean_law

국가법령정보 API를 통해 최신 법령을 실시간으로 조회합니다.

- ✓ 법령, 시행령 및 유권해석 근거 보완

get_news

News API를 활용하여 부동산 시장의 최신 동향을 파악합니다.

- ✓ 실시간 이슈 및 정책 변화 감지

llm_as_a_judge

답변 품질을 0~5점 척도로 자가 평가하여 신뢰도를 검증합니다.

- ✓ GPT-4o-mini 활용 (비용 절감)

check_policy_safety

답변이 정부 정책에 위배되지 않는지 최종 안전성을 검토합니다.

- ✓ 금융/부동산 규제 준수 여부 필터링

get_user_summary

사용자의 장기 기억(선행 지역, 예산, 제약)을 조회합니다.

- ✓ 개인화된 맞춤형 답변 제공

Planner 단계

복잡 질문 처리 (Complex Mode)

APPLIED MODEL

GPT-4o-mini



질문 정제

Query Refining

- ✓ 사용자의 날것의 질문을 명확하게 다듬기
- ✓ 모호한 의도를 파악하여 구체적 표현으로 변환
- ✓ 다음 단계(Tool) 실행을 위한 최적화 수행



도구 계획

Tool Planning

- ✓ 질문 해결에 필요한 Tool 호출 리스트 정리
- ✓ 도구 실행 순서 및 파라미터 정의
- ✓ Planner JSON 포맷으로 구조화된 계획 생성



비용 최적화

Cost Saving

- ✗ Planner의 계획은 세션/히스토리에 저장 안 함
- ✓ 불필요한 컨텍스트 누적 방지로 토큰 비용 절감
- ✓ 일회성 추론 과정으로 처리하여 효율성 극대화



Planner는 오직 '계획 수립'만을 위한 중간 단계이며, 결과물은 히스토리에 쌓지 않아 경제적입니다.

집사부 AI Agent Project

Tool 호출 루프

반복 실행 및 자료 제공 (Execution Loop)

APPLIED MODEL

GPT-4o



1



판단 및 호출

Decision & Call

- ✓ 최대 6회(MAX_TOOL_LOOPS)까지 반복 수행하여 복잡한 작업 처리
- ✓ LLM이 상황에 맞는 도구(tool_calls)를 스스로 선택 및 파라미터 생성
- ✓ 함수 실행 후 결과를 role: tool 메시지로 대화 내역에 기록

2



결과 및 자료

Result & Download

- ✓ 도구 실행 결과(tool_results)를 저장하여 다음 판단의 근거로 활용
- ⬇ RAG 검색된 참고 문서(PDF)
의 다운로드 링크 자동 생성 및 제
공
- ✓ 오류 발생 시 에러 정보를 피드백하여 자가 수정(Self-Correction)

3



답변 확정

Draft Answer

- ✓ 추가 도구 호출이 필요 없으면 최종 답변(draft_answer) 생성
- ✓ 수집된 정보들을 종합하여 사용자 질문에 대한 명확한 해답 구성
- ✓ 근거 자료와 다운로드 링크를 포함한 최종 응답 반환 후 루프 종료



정보가 충분해질 때까지 반복 수행하며, 사용자가 직접 문서를 확인할 수 있도록 원본을 제공합니다.

집사부 AI Agent Project

LLM Judge 평가

답변 품질 관리 및 자가 수정 (Quality Control)

JUDGE MODEL

GPT-4o-mini



1



정량적 평가 수행

0~5 Scale Scoring

- ✓ 생성된 답변을 0점부터 5점까지 척도로 평가
- ✓ 평가 기준: 정확성, 관련성, 근거 문서의 포함 여부
- ✓ 비용 효율적인 GPT-4o-mini가 심사위원 역할 수행

2



통과 여부 판단

Pass / Fail Decision

- ✓ 기준 점수 4점 이상 시 즉시 사용자에게 답변 제공
- ✓ 4점 미만(Fail) 시 구체적인 실패 사유(Reason) 도출
- ✓ 환각(Hallucination) 및 오정보 필터링의 핵심 관문

3



자가 수정 루프

Self-Correction

- ✓ 도출된 Reason을 System 프롬프트에 반영하여 재시도
- ✓ 최대 3회 재생성(Retry) 수행으로 답변 품질 개선
- ✓ 최종 실패 시, 검색된 문서를 기반으로 보수적 답변 제공

사용자 장기기억 시스템

개인화된 맞춤형 답변을 위한 데이터 영속성 관리 (User Memory)

SQLite + Fernet (AES-128)



정보 추출

대화 맥락 분석
답변 생성 직전,
사용자 취향·제약사항
자동 식별



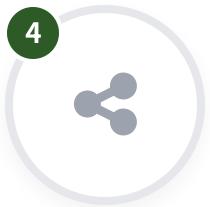
구조화 저장

DB 스키마 매팅
user_id (PK)
summary
date



보안 암호화

AES-128 적용
민감 정보 보호를 위해
Fernet 대칭키로
암호화하여 저장



세션 공유

기억의 연속성
동일 user_id 접속 시
모든 세션 간
장기 기억 공유



툴 정보로 제공

get_user_summary
실시간 복호화 후
Tool 형태로
사용자 정보 제공

사용 시나리오 예시

실제 시스템 동작 화면 (System Demonstration)

SCENARIO
#01 정책 조회

localhost:8501/

전체 대화 화면

DSR 시행방안에 대해 외부문서 조회 사용해서 조회해보고 정리해보기 알려줘

답변 준비가 완료되었습니다.

처리 시간: 약 25.4초

Tool Result: search_vector_store

Tool Result: search_korean_law

"DSR 시행방안"에 관한 정보를 외부 문서를 통해 다음과 같이 확인해드리겠습니다. DSR(총부채원리금상환인의 대출 원리금 상환율)은 소득과 비교하여 평가하는 중요한 지표로, 금융 시장의 안정화를 목표로 합니다.

[핵심 요약]

- DSR의 정의와 필요성: DSR은 대출자의 상환 능력을 평가하여 금융 리스크를 줄이는데 사용됩니다.
- 시행 단계: DSR 제도는 단계적으로 시행되며, 3단계 스트레스 DSR 시행 방안을 통해 강화됩니다.

상세 설명

- DSR의 의미 및 운영
 - DSR (Debt Service Ratio): 연 소득 대비 모든 대출의 연간 원리금 상환액의 비율로, 개인의 채무 상환 능력을 평가하는 지표입니다.
 - 운영: DSR은 대출 심사 시 대출자의 금융 건전성을 확보하는데 중요한 역할을 하며, 대출자의 부채 상황을 고려해 조정합니다.

질문을 입력해 주세요.

로그인 중

1207_064246

1207_063615

1207_040523

상태

문서 청크 수: 233

자료를 기반으로

localhost:8501/

문서 검색 결과 및 다운로드

문서 검색 결과

- Chunk 1 ((250520) (안건) 3단계 스트레스 DSR 시행방안(최종배포본).pdf) (더보기)
- Chunk 2 (250227[별첨] '25년도 가계부채 관리방안.pdf) (더보기)
- Chunk 3 (250227[별첨] '25년도 가계부채 관리방안.pdf) (더보기)
- Chunk 4 (250520(보도자료) 3단계 스트레스 DSR 시행방안 확정.발표.pdf) (더보기)
- Chunk 5 (정책브리핑_251017_주택담보대출관리방안.pdf) (더보기)

이 질문과 관련된 원문 파일 다운로드

- (250520) (안건) 3단계 스트레스 DSR 시행방안(최종배포본).pdf
- 250227[별첨] '25년도 가계부채 관리방안.pdf
- 250520(보도자료) 3단계 스트레스 DSR 시행방안 확정.발표.pdf
- 정책브리핑_251017_주택담보대출관리방안.pdf



시스템 시연

집사부 AI Agent의
실시간 동작 과정을 보여드립니다.

Live Demo



질의 응답

프로젝트에 대해 궁금한 점을
자유롭게 질문해 주세요.

Q&A Session

경청해 주셔서 감사합니다.

2025 LLM & AI Agent Project Final Presentation