



## LLM 이 잘못된 실행을 하지 않도록 시스템을 설계하는 엔지니어 구보은

Birth : 1995.03.31

E-mail : kuk9096@naver.com

Phone : (+82) 010-3521-6973

Github : <https://github.com/koooooooo999>

Address : 인천광역시 부평구 영성중로 16

### Skills

**Backend** : Python, FastAPI, Java, SpringBoot

**AI / ML** : LLM(Claude API, OpenAI, Gemini), LangChain, LangSmith, LangGraph, DeepAgents

**Frontend** : HTML5, CSS, React.js, Next.js

**Database** : MySQL, PostgreSQL

**DevOps & Tools** : Git, GitHub, Aws, GitHub Actions, Docker, draw.io

### 학력

인천대학교 / 법학, 경영(복전) 2015 년 3 월 - 2022 년 8 월

인천영선고등학교/ 졸업 2011 년 3 월 - 2014 년 2 월

### 교육 과정

심화\_생성형 AI 활용 인재양성과정 | 2026.05.15-07.14 | 하이미디어아카데미

AWS 와 Docker & Kubernetes 를 활용한 Java Full-Stack 개발자 양성과정 | 2025.04.30-11.14 | 쌍용교육센터

### 자격증

SQLD, 정보처리기사 필기 합격, 1 종보통 운전면허

### Project

#### AI 광고 비서 에이전트 - [ClickMe](#)

2026.05.27 - 07.14  
(7 주)

#### 개요

AI 시뮬레이션·광고 생성·운영 자동화를 지원하는 광고 AI 플랫폼.

#### 담당 역할

LLM 기반 광고 운영 AI Agent 설계 및 실행 제어 시스템 개발

#### 담당 업무

- LangGraph-DeepAgents 기반 광고 운영 Agent 워크플로우 설계 및 구현
- 위험도 기반 실행 제어(HITL) 및 승인 정책 시스템 구축
- 실행 무결성·명등성 검증 기반 Meta API 집행 파이프라인 구축
- 감사 로그(Audit Trail) 및 실행 이력 관리 체계 구축
- 회귀 테스트 30 건 및 LangSmith 기반 Observability 환경 구축

#### 문제 해결 경험

**배경** : 광고 성과의 감지·진단·조치를 24 시간 자동화하면서, 실제 비용을 움직이는 Meta 광고

---

계정의 변경 권한을 안전하게 통제해야 했음

#### [Meta API 집행-DB 기록 간 중복 집행 방지]

##### 문제

외부 Meta API 호출과 DB 기록을 하나의 트랜잭션으로 처리할 수 없어, 장애나 재시도 시 동일한 작업이 중복 실행될 수 있는 위험 존재

##### 해결

- DB UNIQUE 제약으로 Idempotency Key 기반 실행 예약을 선점하고, 최초 요청만 외부 API 를 호출하도록 구현
- 실행 실패 시 예약 정보를 해제해 정상적인 재시도는 가능하도록 처리
- 외부 API 는 성공했지만 후속 작업이 실패한 경우에는 결과를 기록하고 추가 실행을 차단하도록 설계

##### 결과

동일 요청의 중복 집행을 방지하고, 장애 발생 시에도 일관된 실행 상태를 유지하도록 설계

#### [승인 이후 실행 요청 변조 리스크 차단]

##### 문제

사용자가 승인한 실행 계획과 실제 실행되는 내용이 달라질 수 있는 위험 존재.

##### 해결

- 승인 시점의 실행 계획을 proposal\_hash 로 고정해 변경 여부를 확인하도록 구현
- 실행 직전에 승인 정보와 정책, 권한, 만료 여부를 다시 검증하는 이중 검증 적용
- 예산 값을 정수(KRW)로 통일해 데이터 표현 차이로 검증이 실패하는 문제 방지

##### 결과

승인된 실행 계획만 실제 실행되도록 보장해 실행 무결성을 확보

## 이러닝 프로젝트 - [CodeBlock](#)

### 개요

IT 학습 콘텐츠 수강, 결제, 수강권 관리를 제공하는 이러닝 플랫폼

### 담당 역할

Spring Boot 기반 결제 승인·환불 파이프라인 및 결제 정책 엔진 개발

### 담당 업무

- TossPayments 연동 결제 승인·취소 파이프라인 구현 (승인·웹훅 수신·취소 및 응답 매핑), 웹훅에 서명 검증과 중복 차단 적용
- 외부 승인 호출을 트랜잭션 밖으로 분리한 2 단계 결제 흐름(prepare-confirm) 설계
- 결제 전 검증을 금액·적립금 잔액·일일 한도·먹등키 등 7 개로 분리하고, 외부 승인 이전 트랜잭션에 배치
- 먹등성 키 UNIQUE 제약과 비관적 락 기반 중복 결제·동시 요청 차단
- 환불 후처리(수강권·섹션 소유권 회수, 적립금·쿠폰 복원, 정산 제외, 주문 확정) 자동화 및 실패 단계 재개 배치 구현
- 환불 가능 기간 동안 강사 지급을 보류하는 정산 원장 상태 설계
- 조회 전용 모델 분리 리팩토링, 동시성·조회 분리 회귀 포함 테스트 74 건 작성

### 문제 해결 경험

배경 : 롤백 불가능·응답 불확실한 외부 PG 와 내부 결제 도메인 간 돈·권한 정합성 확보

#### [승인 응답 유실 시 판단 기준 설계]

#### 문제

승인 요청이 타임아웃되면 실제 결제 집행 여부를 알 수 없음. 미집행으로 판단했으나 실제로는 집행된 경우, 취소 대상을 잃은 채 청구만 남는 위험 존재

#### 해결

- 타임아웃과 5xx 를 결과 불명 상태로 분류하고, 승인 식별자를 보존해 상태 조회 또는 보상 취소가 가능하도록 설계
- 예외에 포함된 승인 식별자를 결제 기록에 저장해 취소 대상을 유실하지 않도록 처리
- 미집행 건의 취소 요청은 '이미 취소됨'으로 응답되므로 이를 성공으로 흡수

#### 결과

오픈 비용이 한쪽으로만 발생하도록 설계해, 잘못 판단해도 불필요한 취소 요청 1 회로 종료

## [결제 실패 시 쿠폰 유실 방지 — 예약 상태머신 설계]

### 문제

결제 중 쿠폰을 즉시 사용 처리하면 결제 실패 시 쿠폰이 사용된 상태로 남는 문제

### 해결

- 쿠폰 상태를 AVAILABLE → RESERVED → USED 로 분리하는 상태머신 설계
- 결제 완료 시 사용 확정, 실패 시 자동 복원되는 예약 처리 구조 구현
- 실제 결제 금액 기준 환불 정책을 적용해 할인 금액의 현금 환불 방지

### 결과

결제 실패 시 쿠폰 유실을 방지하고, 쿠폰과 결제 데이터의 정합성 확보

## [환불 후처리 부분 실패 대응]

### 문제

환불은 결제 취소·수강권 회수·적립금 복원·쿠폰 복원·정산 제외·주문 확정으로 이어지는 다단계 처리. 단일 트랜잭션으로 묶으면 후반 실패가 앞 단계의 성공까지 롤백시키고, 앞에서 중단되면 정산 제외가 누락되어 환불된 금액이 강사에게 지급되는 문제 발생

### 해결

- 외부 결제 취소는 성공했지만 DB 후처리 트랜잭션이 롤백되어 외부 결제 상태와 내부 상태가 불일치할 수 있음
- 한 단계가 실패해도 나머지 단계는 계속 진행되도록 설계
- 실패로 남은 단계는 5 분 주기 배치가 최대 5 회까지 재시도

### 결과

부분 실패가 소실되지 않고 데이터로 남아 추적 가능하며, 사람의 개입 없이 자동 재개

---