

익명 상담 메신저 앱 프로젝트 제안서

LLM 기반 스마트 라우팅 시스템을 갖춘
학생-교수 익명 소통 플랫폼

프로젝트명	익명 상담 메신저 (가칭: AnonCounsel)
개발 환경	Android Studio (Java)
개발 기간	6개월 (2025.11 ~ 2026.05)
작성일	2025년 11월 22일

목차

1. 프로젝트 개요
2. 배경 및 필요성
3. 핵심 기능
4. 기술 스택
5. 시스템 아키텍처
6. 보안 설계
7. LLM 활용 방안
8. 개발 일정
9. 기대 효과
10. 결론

1. 프로젝트 개요

1.1 프로젝트 소개

본 프로젝트는 학생들이 교수 및 조교와 익명으로 안전하게 소통할 수 있는 모바일 메신저 애플리케이션 개발을 목표로 합니다. Large Language Model(LLM)을 활용한 지능형 라우팅 시스템을 통해 민원 내용을 자동으로 분석하고, 적절한 상담자를 추천하여 효율적인 소통 경로를 제공합니다.

1.2 핵심 가치

핵심 가치	설명
완전한 익명성	학생의 신원을 보호하면서도 양방향 소통 가능
지능형 라우팅	LLM 기반 민원 분석으로 최적의 상담자 자동 추천
철저한 보안	암호화 통신 및 자동 파기 시스템으로 프라이버시 보호
편리한 아카이빙	로컬 저장으로 개인 기록 관리 및 증거 보관

2. 배경 및 필요성

2.1 현재 문제점

- 신원 노출 우려: 이메일이나 대면 상담 시 학생의 신원이 노출되어 불이익에 대한 두려움으로 솔직한 소통이 어려움
- 일방향 소통의 한계: 익명 설문이나 건의함은 답변을 받을 수 없어 실질적인 문제 해결이 불가능
- 공개로 인한 2차 피해: 대나무숲 등 공개 플랫폼은 민원 내용이 노출되어 특정 가능성 존재
- 비효율적인 전달 경로: 학생들이 누구에게 문의해야 할지 몰라 잘못된 경로로 민원을 제기하는 경우 발생

2.2 해결 방안

본 프로젝트는 위의 문제점들을 해결하기 위해 다음과 같은 핵심 기능을 제공합니다:

- 완전한 익명성을 보장하면서도 교수/조교와 양방향 소통 가능
- LLM 기반 자동 분석으로 적절한 상담자에게 자동 라우팅
- 1:1 비공개 소통으로 프라이버시 완벽 보호
- 일정 기간 후 서버 데이터 자동 파기로 장기 보관 리스크 제거
- 로컬 아카이빙으로 필요시 증거 자료로 활용 가능

3. 핵심 기능

3.1 완전 익명 메시징 시스템

학생은 실명 없이 고유한 익명 ID를 통해 상담을 진행합니다. 교수/조교는 학생의 신원을 알 수 없으며, 답장 시에도 익명성이 유지됩니다.

3.2 LLM 기반 스마트 라우팅

민원 작성 시 LLM이 텍스트를 분석하여 다음 정보를 추출합니다:

- 카테고리 분류: 수강 문의, 성적 관련, 학업 상담, 개인 고민, 긴급 신고 등
- 감정 분석: 일반, 불만, 긴급 등의 우선순위 판단
- 키워드 추출: 주요 내용 파악 및 검색 가능성 제공
- 추천 수신자: 내용에 가장 적합한 교수/조교 자동 추천

3.3 보안 및 프라이버시 보호

- 엔드투엔드 암호화: 메시지 내용은 발신자와 수신자만 확인 가능
- 자동 파기 시스템: 서버에 저장된 메시지는 30일 후 자동 삭제
- 메타데이터 최소화: IP 주소, 디바이스 정보 등 개인 식별 정보 미수집
- 로컬 아카이빙: 사용자 디바이스에만 암호화 저장되어 필요시 증거로 활용

3.4 직관적인 사용자 경험

- 간편한 민원 작성 인터페이스 (텍스트, 파일 첨부 지원)
- 실시간 푸시 알림으로 답장 확인
- 대화 내역 관리 및 검색 기능
- 카테고리별 분류 및 필터링
- 다크 모드 및 접근성 지원

4. 기술 스택

4.1 개발 환경

구분	기술
언어	Java (JDK 11+)
IDE	Android Studio
최소 SDK	API 26 (Android 8.0)
타겟 SDK	API 34 (Android 14)
아키텍처	MVVM Pattern

4.2 핵심 라이브러리

분류	라이브러리	용도
UI/Architecture	AndroidX, Lifecycle, RecyclerView	MVVM 패턴 구현, 생명주기 관리, 리스트 표시
Database	Room Database	로컬 데이터 암호화 저장
Network	Retrofit 2, OkHttp 3	REST API 통신, HTTP 클라이언트
Backend	Firebase (Firestore, Authentication, Cloud Messaging, Cloud Functions)	실시간 데이터베이스, 인증 관리, 푸시 알림, 서버 로직
Cryptography	Bouncy Castle, Android Keystore	RSA, AES 암호화, 키 안전 보관
LLM Integration	Anthropic API (Claude)	민원 분석 및 라우팅

5. 시스템 아키텍처

5.1 MVVM 아키텍처

프로젝트는 MVVM (Model-View-ViewModel) 패턴을 채택하여 관심사의 분리와 유지보수성을 확보합니다.

- **Model:** 데이터 클래스 및 비즈니스 로직 (Message, User, Recipient 등)
- **View:** Activity/Fragment를 통한 UI 표시 및 사용자 입력 처리
- **ViewModel:** UI 로직과 데이터 바인딩, LiveData를 통한 반응형 업데이트
- **Repository:** 데이터 소스 추상화 (로컬 DB, 원격 API, LLM 서비스)

5.2 메시지 전송 플로우

1. 학생이 민원 내용 작성 및 전송 버튼 클릭
2. LLM API 호출하여 카테고리, 감정, 추천 수신자 분석
3. 분석 결과를 사용자에게 표시하고 최종 수신자 선택
4. 익명 ID 생성 (UUID 기반)
5. 메시지를 AES-256으로 암호화
6. 수신자 공개키(RSA)로 AES 키 암호화
7. 암호화된 데이터를 Firebase Firestore에 저장
8. FCM을 통해 수신자에게 푸시 알림 전송
9. 로컬 Room DB에 발신 내역 암호화 저장

5.3 자동 파기 시스템

Firebase Cloud Functions를 활용하여 서버에 저장된 메시지를 30일 후 자동으로 삭제합니다. 이를 통해 장기 보관으로 인한 프라이버시 침해 위험을 원천적으로 차단합니다. 사용자가 필요한 경우 로컬 디바이스에 암호화된 상태로 보관하여 증거 자료로 활용할 수 있습니다.

6. 보안 설계

6.1 하이브리드 암호화

효율성과 보안성을 동시에 확보하기 위해 대칭키 암호화(AES)와 공개키 암호화(RSA)를 결합한 하이브리드 방식을 채택합니다.

- **AES-256-GCM**: 실제 메시지 내용을 빠르게 암호화 (대칭키 암호화)
- **RSA-2048**: AES 키를 수신자 공개키로 암호화 (비대칭키 암호화)
- **Android Keystore**: 개인키를 안전하게 보관 (하드웨어 기반 보안)
- **SHA-256**: 익명 ID 해싱 및 메시지 무결성 검증

6.2 익명성 보장 메커니즘

- **익명 ID**: 매 세션마다 새로운 UUID 생성, 실명 정보 미저장
- **메타데이터 최소화**: IP 주소, MAC 주소, 디바이스 ID 수집 안 함
- **타임스탬프 라운딩**: 정확한 시간 대신 5분 단위로 반올림하여 저장
- **파일 크기 패딩**: 첨부 파일의 실제 크기를 숨기기 위한 패딩 추가
- **EXIF 제거**: 사진 첨부 시 위치 정보 등 메타데이터 자동 삭제

6.3 위협 모델 및 대응

위협	대응 방안
서버 해킹	E2EE로 암호화된 데이터만 존재, 평문 노출 불가
네트워크 도청	TLS 1.3 + E2EE 이중 암호화
내부자 공격	서버 관리자도 내용 확인 불가능
메타데이터 분석	최소 수집 및 라운딩으로 패턴 분석 차단
디바이스 분실	Room DB 암호화 + 생체 인증으로 보호

7. LLM 활용 방안

7.1 Claude API 선택 이유

- 한국어 지원: GPT 대비 우수한 한국어 이해 및 생성 능력
- 긴 컨텍스트: 200K 토큰으로 긴 민원도 충분히 분석 가능
- 안전성: Constitutional AI로 유해 콘텐츠 필터링 우수
- **API** 안정성: 기업용 API 제공으로 안정적인 서비스
- 비용 효율: 합리적인 가격 정책 (학생 프로젝트에 적합)

7.2 LLM 분석 기능

민원 텍스트를 Claude API에 전송하여 다음 정보를 추출합니다:

분석 항목	예시	활용
카테고리	수강문의, 성적, 학업상담, 개인고민, 긴급신고	적절한 수신자 그룹 필터링
감정/긴급도	일반, 불만, 긴급, 응급	우선순위 설정 및 알림
핵심 키워드	시험, 과제, 출석, 학점 등	검색 및 통계 분석
추천 수신자	담당교수, 학과조교, 학생처 등	최적 상담자 자동 매칭

7.3 LLM 사용 시 프라이버시 고려사항

민원 내용을 외부 LLM API로 전송하므로 프라이버시 보호가 중요합니다. 다음과 같은 조치를 취합니다:

- 사용자 동의: LLM 분석 사용에 대한 명시적 동의 획득
- 데이터 최소화: 분석에 필요한 텍스트만 전송, 메타데이터 제외
- **Zero Data Retention:** Anthropic의 ZDR 정책 활용 (학습 데이터로 미사용)
- 로컬 옵션: 향후 온디바이스 LLM(Gemini Nano 등)으로 전환 가능
- 선택적 사용: 사용자가 LLM 분석을 거부하고 수동 선택 가능

8. 개발 일정

6개월 개발 기간을 3개의 단계(Phase)로 나누어 단계적으로 기능을 구현합니다.

Phase 1: 기본 기능 구현 (1-2개월)

- 프로젝트 세팅 및 개발 환경 구축
- UI/UX 설계 및 와이어프레임 작성
- MVVM 아키텍처 기본 구조 구현
- Firebase 프로젝트 설정 및 연동
- 익명 ID 생성 및 관리 시스템
- 기본 메시징 기능 (텍스트 전송/수신)
- 푸시 알림 (FCM) 구현
- 로컬 DB (Room) 설정

Phase 2: 보안 및 LLM 통합 (2-3개월)

- RSA 키 쌍 생성 및 관리
- AES-256 대칭키 암호화 구현
- 하이브리드 암호화 시스템 완성
- Claude API 연동 및 프롬프트 엔지니어링
- LLM 기반 카테고리/감정 분석 기능
- 추천 수신자 알고리즘 구현
- 메타데이터 최소화 및 익명성 강화
- EXIF 제거 기능 (사진 첨부)
- 통합 테스트 및 버그 수정

Phase 3: 고급 기능 및 완성도 (1-2개월)

- Firebase Cloud Functions로 자동 파기 시스템 구현
- 로컬 아카이빙 및 PDF 내보내기 기능

- 검색 및 필터링 기능
- 다크 모드 및 접근성 지원
- 관리자 대시보드 (통계만, 내용 비공개)
- 성능 최적화 및 배터리 절약
- 보안 감사 및 취약점 점검
- 사용자 테스트 및 피드백 반영
- 최종 테스트 및 문서화
- 발표 자료 준비

개발 일정 요약

단계	기간	주요 마일스톤
Phase 1	1-2개월 (2025.11-12)	기본 메시징 완성
Phase 2	2-3개월 (2026.01-03)	보안 + LLM 통합
Phase 3	1-2개월 (2026.04-05)	자동 파기 + 완성도

9. 기대 효과

9.1 기술적 학습 성과

- 모바일 앱 개발 경험: Android 플랫폼 전반에 대한 깊이 있는 이해
- 보안 기술: 실무 수준의 암호화 시스템 설계 및 구현 능력
- 클라우드 통합: Firebase를 활용한 백엔드 아키텍처 설계
- **AI/LLM** 활용: 최신 생성형 AI를 실제 프로젝트에 통합하는 경험
- 소프트웨어 공학: MVVM 패턴, Clean Architecture 등 설계 원칙 적용

9.2 실용적 가치

본 프로젝트는 단순한 학습용 프로토타입이 아닌, 실제 학교 현장에서 사용 가능한 실용적인 솔루션입니다.

- 학생 보호: 익명성 보장으로 학생들의 솔직한 소통 유도 및 불이익 방지
- 효율적 상담: LLM 라우팅으로 잘못된 경로로 인한 시간 낭비 감소
- 증거 보존: 로컬 아카이빙으로 필요시 법적 증거 자료로 활용 가능
- 확장 가능성: 다른 교육 기관, 기업 내부 신고 시스템으로 확장 가능
- 오픈소스화: 코드 공개로 다른 개발자들의 학습 자료 제공

9.3 사회적 영향

- 학생 인권 보호 및 안전한 학습 환경 조성
- 교수-학생 간 신뢰 기반 소통 문화 구축
- 학교 폭력, 성희롱 등 심각한 문제의 조기 발견 및 대응
- 디지털 프라이버시 보호의 모범 사례 제시
- 학생 개발자의 사회 기여 프로젝트 사례

9.4 포트폴리오 가치

본 프로젝트는 취업 및 대학원 진학 시 다음과 같은 강점을 어필할 수 있습니다:

- 최신 기술 트렌드 (LLM, E2EE)를 실제 프로젝트에 적용한 경험
- 사회적 문제 해결에 대한 고민과 실천력

- 보안을 고려한 시스템 설계 능력
- 6개월의 장기 프로젝트 완수 경험
- 실제 사용자를 위한 UX 설계 및 구현

10. 결론

본 프로젝트는 학생들이 교수 및 조교와 안전하게 소통할 수 있는 익명 상담 메신저 앱을 개발하여, 학내 소통 문화를 개선하고 학생 인권을 보호하는 것을 목표로 합니다.

특히 Large Language Model(LLM)을 활용한 지능형 라우팅 시스템은 단순한 메신저를 넘어 효율적이고 맞춤형 상담 경험을 제공합니다. 엔드투엔드 암호화, 자동 파기 시스템, 로컬 아카이빙 등 철저한 보안 설계를 통해 사용자의 프라이버시를 최우선으로 보호합니다.

6개월의 개발 기간 동안 단계적으로 기능을 구현하여 완성도 높은 애플리케이션을 만들고, 이를 통해 안드로이드 개발, 보안 기술, AI 통합 등 다양한 기술적 역량을 습득할 것입니다.

본 프로젝트는 단순한 학습용 프로토타입이 아닌, 실제 학교 현장에서 사용 가능한 실용적인 솔루션이며, 향후 다른 교육 기관이나 조직으로 확장할 수 있는 확장성을 갖추고 있습니다.

핵심 가치 요약

혁신성	LLM 기반 스마트 라우팅
보안성	엔드투엔드 암호화 + 자동 파기
실용성	실제 사용 가능한 솔루션
확장성	다양한 조직으로 확장 가능
학습 가치	최신 기술 스택 종합 경험

본 제안서에 기반하여 체계적이고 안정적인 개발을 진행하겠습니다.