Team 31

EV-DLP

임베딩 벡터 기반 데이터 유출 방지 솔루션

지도교수: 윤명근
팀원: 조항범, 김민승, 박찬민, 백승렬, 심지아, 오주엽

Embedding Vector based Data Leakage Prevention

임베딩 벡터 기반의 의미론적 유사도 기술을 사용하여 문서 간 유사도를 효과적으로 비교하고
생성형 AI 질의를 통한 기밀 유출 위험 쿼리를 식별하고 내부 기밀 정보 유출을 실시간 방어합니다.

개발 배경

문제 상황 1: 생성형 AI로 인한 조직의 기밀 유출 사고 증가

문제 상황 2: 기존 유사도 비교 방식의 탐지 한계점

문제 상황 3: 기밀 유출 현황 파악 필요성 증가

문제 상황 4: 기밀 유출 우려로 생성형 AI 활용 어려움

↓

의미론적 유사도를 기반으로 기밀 유출 위협을 **실시간 탐지**
+
Web 플랫폼을 통해 기밀 유출 현황 시각화

핵심 기능

의미론적 유사도 비교

형태론적 유사도 비교가 아닌, 의미론적 유사도를 비교하여 다양한 변형 기밀 정보 유출 시도를 효과적으로 대응함

유출 위험 쿼리에 대한 처리

조직 내부의 규칙에 따라 기밀 유출 위험 쿼리에 대해 조직 내부의 Private LLM을 통해 제한된 답변을 생성하거나, 외부 Open LLM에게 전달을 차단함

유출 현황 시각화

조직의 관리자에게 기밀 파일을 관리하는 기능을 제공하고,조직의 기밀 유출 현황 통계 자료를 시각화하여 효율적으로 조직의 기밀 정보 관리가 가능하도록 함

결과 & 기대효과

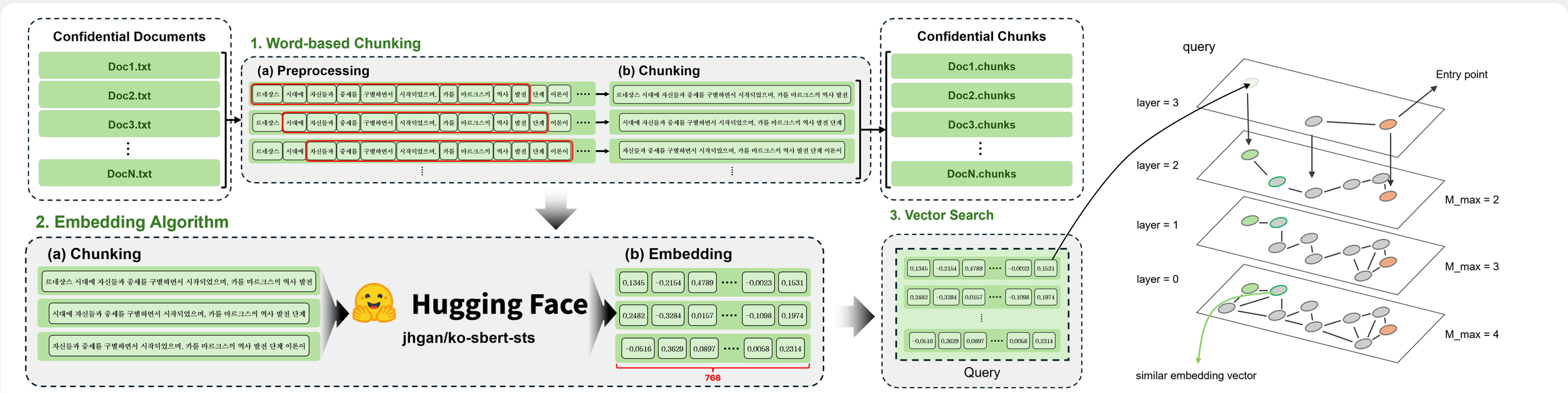
형태론적 유사도의 낮은 정확도 극복

빠른 연산 시간을 통한 대량의 질의 대응 가능

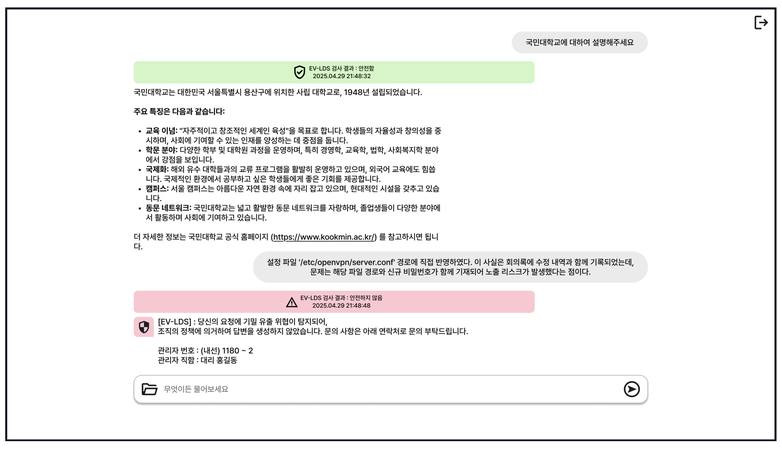
생성형 AI를 통한 내부 정보 유출 실시간 위험 감지 가능성 제시

조직 내 안전한 생성형 AI 기술을 통한 업무 효율 극대화

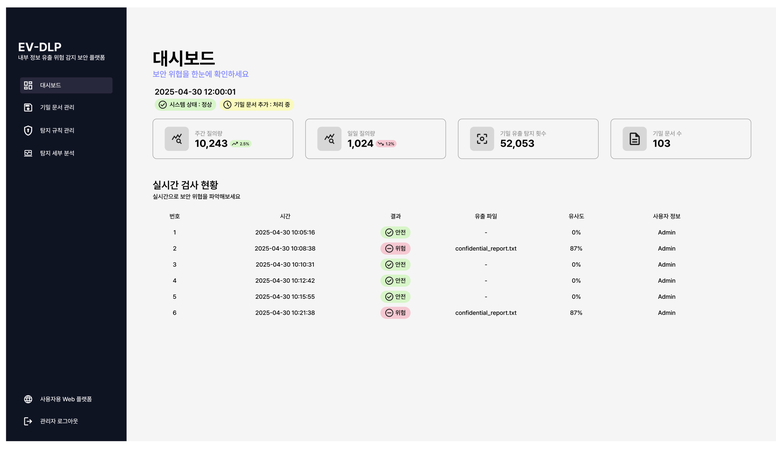
구조도



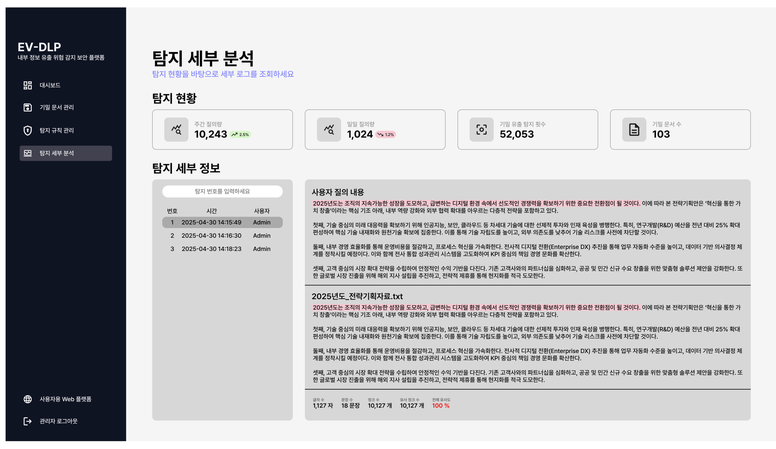
주요 기능



- 사용자 질의에 대해 기밀 유출 위험 검사
- 검사 결과 기밀 유출이면 응답 거부



- 기밀 유출 현황을 대시보드를 통해 시각화
- 실시간 검사 현황 제공



- 기밀 유출 세부 로그 제공
- 유사한 문맥을 지닌 청크 시각화