Q. LLM과 통신 구간에 대한 보안 처리는 어떤 방식이 있는가?

A. 앞에 서비스 단계 WEB / WAS 단계 통신에 대한 암호화 및 권한, 인증 통제등으로 보안을 강화하고 데이터에서 민감정보에 대한 표현을 통제 하는 방식으로 하고 있습니다.

6.2 문서 및 접근 권한 제어

#권한제어 #RBAC #버전관리 #문서보안

Q. 전자 문서들에 대한 검색 권한 반영한 검색 처리는 어떻게 하는지?

A. 수집 단계에서 문서의 권한 관리 인덱스를 별도로 구성합니다.

조회 할 때 자주 변경되고 업데이트 되는 권한을 감안하여 처리하는 부분은 성능이 매우 떨어지는 부분이 있었습니다. 권한 인덱스에서 권한 처리를 먼저 조회 확인 후 데이터를 조회해서 가저오는 두번 쿼리 하는 방식으로적용하는것이 경험상 가장 잘 되어서, 삼성전자에서도 이러한 방식 적용하여 프로젝트를 진행하였습니다

Q. RAG 시스템 내 권한 관리는 어떤 식으로 이루어지는가? (관리자, 사용자)

A. RAG 시스템에서는 RBAC, 즉 역할 기반 접근 제어 방식을 채택하여 권한을 관리합니다.

이 방식에서는 권한을 사용자에게 직접 부여하지 않고, 역할 단위로 먼저 권한을 정의한 다음, 사용자가 해당 역할을 갖도록 설정합니다. 예를 들어, 관리자 역할에는 문서 색인, 삭제, 로그 조회 등의 권한이 포함되고, 일반 사용자 역할에는 문서 검색 및 조회만 포함됩니다.각 사용자는 하나 이상의 역할을 가질 수 있으며, 역할 변경 시 자동으로 권한 범위가 조정되므로 유지보수가 용이합니다.

Q. RAG에서 접근권한에 따라 답변은 어떻게 출력되는가?

A.사용자가 검색이나 챗봇 질의를 수행할 경우, 시스템은 먼저 해당 사용자의 권한 정보를 확인한 후, 접근 가능한 문서만을 검색 대상으로 삼습니다.

이 과정을 통해 답변 생성 시 참조되는 문서는 모두 사용자에게 허용된 범위 내에 있는 것들로 제한되며, 권한이 없는 문서의 내용은 시스템적으로 아예 접근할 수 없도록 필터링됩니다.