Journal of KIIT. Vol. 23, No. 9, pp. 173-179, Sep. 30, 2025. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2025.23.9.173

기업용 RAG 시스템의 보안 강화를 위한 ACL 기반 모델

이 이 섭*

ACL-based Model for Enhancing the Security of Enterprise RAG Systems

Lee-Sub Lee*

본 연구는 국립금오공과대학교 교수연구년제에 의하여 연구된 실적물

요 약

본 논문은 기업 내부에서 사용하는 RAG(Retrieval-Augmented Generation) 시스템의 보안성을 강화하기 위해 ACL(Access Control List)를 적용하는 방법을 제안하고, 모델의 안정성을 위협 모델을 통해 검증하였다. RAG 시스템은 공개된 지식 소스에서 정보를 검색하고 이를 생성 모델과 결합하여 사용자에게 필요한 정보를 제공하는 기술로, 기업 내부의 민감한 데이터를 다룰 때 보안 문제가 발생할 수 있다. 본 연구에서는 ACL을 활용하여 사용자 권한에 따라 접근을 제어하는 보안 모델을 설계하였다. 제안된 보안 모델에서 여러 위협을 정의하고 이를 방어하는 방식으로 데이터의 무결성, 기밀성, 접근 제어의 완결성을 검증하였다. ACL을 적용한 RAG 시스템은 데이터 접근 보안성을 크게 향상해, 보안 위협에 효과적으로 대응하는 것으로 나타났다. 본 연구는 기업 환경에서 민감한 정보를 다루는 RAG 시스템의 보안 문제를 해결하기 위한 효과적인 방안을 제시하였다.

Abstract

This paper proposes a method to enhance the security of Retrieval-Augmented Generation (RAG) systems used within organizations by applying Access Control Lists (ACLs), and validates the model's stability through threat modeling. The RAG system retrieves information from publicly available knowledge sources and combines it with a generation model to provide users with the information they need. However, security issues can arise when handling sensitive data within corporate environments. In this study, a security model was designed using ACLs to control access based on user permissions. The proposed security model defines various threats and verifies the integrity, confidentiality, and completeness of access control by defending against them. The RAG system with ACLs significantly enhances data access security and effectively responds to security threats. This research presents an effective solution to address the security issues of RAG systems handling sensitive information in corporate environments.

Keywords

retrieval-augmented generation, RAG, access control list, ACL, data security, threat modeling

* 국립금오공과대학교 컴퓨터공학부 교수
- ORCID: https://orcid.org/0000-0002-0911-2469

· Received: Jun. 17, 2025, Revised: Aug. 06, 2025, Accepted: Aug. 09, 2025
· Corresponding Author: Lee-Sub Lee
Dept. of Computer Engineering, Kumoh National Institute of Technology, Gumi, Korea
Tel.: +82-54-478-7532, Email: eesub@kumoh.ac.kr

Ⅰ. 서 론

최근 외부 지식 소스(Knowledge source)로부터 최신 정보를 추출하고 이를 기반으로 유용한 결과를 생성하는 기술로 RAG(Retrieval Augmented Generation) 시스템이 주목받고 있다[1]. RAG 시스템은 검색과 생성 기능을 결합하여 사용자의 요구에 맞는 최신 정보를 효과적으로 제공할 수 있으며, 지식 기반 시스템의 새로운 패러다임으로 부상하고 있다. 이러한 특성 덕분에 RAG 시스템은 지식 관리, 고객 서비스, 데이터 분석 등 다양한 비즈니스 환경에서 활용 가능성이 크다[2][3].

그러나 기업 내부의 민감한 지식 소스를 활용하는 과정에서 보안 문제가 발생할 수 있다. 특히, 불법적인 민감 정보가 포함되는 정보 유출의 위험이 존재하며[4], 기업에서는 내부 데이터베이스, 벡터 데이터베이스, 문서 저장소 등 다양한 형태의 지식 소스를 사용하고 있으며, 이러한 지식 소스를 기반으로 정보를 추출하고 결과를 생성하는 과정에서 비인가 접근이나 정보 유출의 위험이 발생할 수 있다. 최근 RAG 모델과 LangChain 프레임워크를 적용한 도메인 특화 AI 시스템 연구[5]에서도 외부 데이터와의 통합 과정에서 보안에 대한 고려가 필요함을 시사하고 있다. 특히 기존 연구는 RAG 시스템의 성능 및 정확도 향상에 초점을 맞추고 있어, 실제 환경에서 요구되는 접근 제어나 데이터 보호 기능에 관련된 보안 요건에 대한 논의는 상대적으로 부족한 실정이다. 따라서 RAG 시스템에 대한 보안 기능, 특히 접근 제어와 데이터 보호 메커니즘의 도입이 필수적이다[6][7]. S. Zeng et al.[4]는 개인 식별 정보가 포함된 응답 비율이 20%를 초과한 사례를 보고하였다.

기업 내부의 다양한 지식 소스들은 잘 정의된 ACL(Access Control List) 정책에 의하여 운영되고 있으며, RAG의 통합을 위해 새로운 보안 정책을 수립하고, 구축하고, 운영하는 것은 매우 큰 비용을 요구한다[8]. 따라서 기존의 ACL 정책을 RAG 시스템과 효과적으로 통합하여 검색된 정보가 사용자 권한에 따라 필터링되도록 설계되는 것이 바람직하다[9][10]. 또한, 철저한 접근 제어 및 데이터 유출 방지 메커니즘을 통해 보안성을 강화하고, 무단 접근 위험을 최소화함으로써 RAG 시스템의 안전성과 운영 효율성 향상을 기대할 수 있다.

본 연구에서는 다양한 지식 소스를 일관되게 연동하기 위한 공통 인터페이스를 제안하고, 이를 RAG 시스템에 적용하여 사용자 접근 권한 기반의 응답 필터링을 지원하는 방법을 제시한다. 제안된 방식은 기존 ACL 정책을 수정하지 않고도 RAG 시스템과의 통합이 가능하도록 설계되었으며, 이를 통해 시스템의 보안을 강화하면서도 연동성과 확장성을 확보하였다. 또한, 제안된 보안 모델의 신뢰성을 입증하기 위해 논리적 모델에 위협 모델을 적용하여 검증을 수행하고, ACL 기반 접근 제어가 요구되는 보안 특성을 충족함을 확인하였다.

기존 연구와 달리 본 논문은 실제 정책을 적용할 수 있는 구조적 보안 모델을 제안한다는 점에서 기술적 기여가 있다. 이후 ACL 기반 아키텍처와 위협 모델을 중심으로 보안성 검증을 수행하고, 연구 결과 및 한계점을 논의한다.

본 논문은 ACL을 기반으로 RAG 시스템의 보안성을 강화하는 구조적 방안을 제안한다.

Ⅱ. 관련 연구

2.1 공개형 RAG 시스템

RAG 시스템은 활용하는 지식 소스에 따라 공개된 외부 지식 소스를 활용하는 경우와 기업 내부의 지식 소스를 사용하는 방식으로 구분될 수 있다. 검색엔진과 같은 외부 지식 소스를 사용하는 RAG 시스템은 공개된 문서 저장소를 기반으로 최신 정보를 반영하고 광범위한 데이터를 제공할 수 있다. 그림 1은 외부 지식 소스를 사용하는 공개형 RAG 시스템의 구성 요소와 데이터 흐름을 설명한다.

그림에서 사용자가 질의를 입력하면, 리트리버가 이를 받아 외부 지식 소스에서 조회를 실행한다. 지식 소스는 관련 문서 목록을 리트리버에게 반환하고, 리트리버는 이를 바탕으로 프롬프트를 구성한다. 이 프롬프트는 LLM(Large Language Model)에 전달되어 최종 답변을 생성한다. 지식 소스의 경우

외부에 이미 공개되어 있기 때문에 별도의 권한 관리의 필요가 없다. 여기에서의 지식 소스는 주로 웹 페이지가 된다.

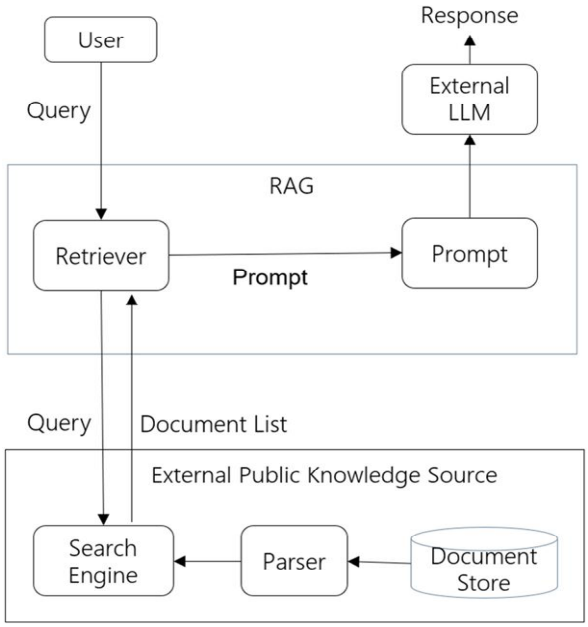

그림 1. 공개형 RAG 모델의 구조
Fig. 1. Architecture of the public RAG system

2.2 ACL과 폐쇄형 RAG 시스템

ACL은 컴퓨터 시스템에서 사용자의 자원에 접근 권한을 관리하는 접근 제어 방식이다. ACL은 파일과 같은 객체에 대해 누가 어떤 행위(읽기, 쓰기, 수정, 삭제 등)를 할 수 있는지를 명시적으로 정의한 목록으로 구성된다. 예를 들어, 한 문서에 대해 특정 부서 직원은 읽기 권한을 갖고, 관리자만 수정 및 삭제 권한을 갖도록 설정할 수 있다.

ACL은 전통적인 운영체제, 데이터베이스 시스템, 웹 애플리케이션, 문서 관리 시스템(DMS) 등에서 광범위하게 활용되며, 세밀한 권한 설정이 가능하다는 장점이 있다. 기업 환경에서 RAG 시스템을 운영할 경우, 민감한 내부 문서가 포함된 지식 소스에 대한 접근 통제를 위해 ACL 기반의 접근 제어가 필수적이다. 그러나 사용자 수가 많거나 권한 구조가 복잡한 경우, ACL의 구축과 관리가 어렵고 큰 비용이 요구된다는 한계가 있다. 이러한 복잡성으로 인해 ACL은 세심하게 관리되어야 한다.

폐쇄형 RAG 시스템은 공개된 외부 데이터가 아닌, 기업 내부의 핵심 정보를 다루기 때문에 권한이 없는 정보는 검색 결과에서 제외되어야 하며, 응답 생성을 위한 프롬프트에 포함되지 않아야 한다. RAG 시스템은 지식 소스에 대해 읽기(Read) 연산만 수행하므로, 접근 제어 정책 역시 사용자가 해당 문서를 읽을 수 있는지만 판단하면 충분하다. 이러한 특성으로 인하여 접근 제어 모델이 ACL, RBAC(Role-Based Access Control), ABAC (Attribute-Based Access Control) 중 어떤 방식을 따르더라도 최종적으로는 사용자가 자원에 접근 가능한가에 대한 판단으로 수렴된다. 따라서 본 논문은 ACL 기반 접근 제어 구조를 채택하면서도, 외부 모듈(예: 어댑터 또는 리트리버)이 사용자 속성이나 역할 정보를 입력으로 받아 조건을 평가함으로써, RBAC 및 ABAC 정책의 결과를 반영하는 방식으로 확장할 수 있도록 설계하였다. 이러한 구조는 기존 ACL 시스템의 단순성과 효율성을 유지하면서도, 보다 유연한 정책 기반 접근 제어 요구를 수용할 수 있다.

본 연구는 이러한 ACL 기반의 폐쇄형 RAG 시스템을 설계하고, 시스템의 보안성을 위협 모델을 통해 검증하고자 한다.

III. ACL 기반 RAG 보안 모델

3.1 폐쇄형 RAG 시스템의 구성 요소

본 절에서는 앞서 설명한 내부 지식 소스의 ACL 적용 구조를 기반으로, 해당 지식 소스들이 RAG 시스템과 통합되어 작동하는 폐쇄형 RAG 시스템의 모델을 제안한다.

그림 2는 기업 내부 환경을 가정하여, ACL 정책이 적용된 다양한 지식 소스와 RAG 시스템이 결합한 문서의 필터링 과정을 나타낸다. 해당 시스템의 동작 절차는 다음과 같다. 사용자가 자연어로 질의를 입력하면, 해당 질의는 리트리버(Retriever) 모듈로 전달된다. 리트리버는 내부에 존재하는 복수의 지식 소스를 대상으로 사용자 정보를 포함하는 질의를 수행하며, 이때 각 지식 소스는 독립적으로 정의된 ACL 정책을 기반으로 사용자 권한에 따라 검색 결과 문서들을 필터링한다. 이렇게 필터링된 검

색 결과는 리트리버에 다시 전달되며, 외부 LLM으로 전달되어 자연어 응답이 생성되며, 최종적으로 사용자에게 결과가 제공된다.

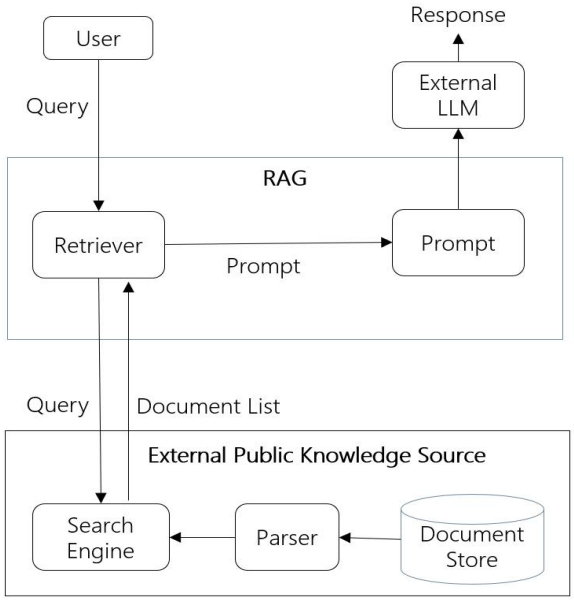

그림 2. 사용자 권한 기반 문서 필터링 과정
Fig. 2. Document filtering process based on user permissions

3.2 폐쇄형 내부 지식 소스

기업 내부에서는 다양한 포맷과 접근 제어 방식이 혼재된 지식 소스들은 활용하게 된다. 이러한 지식 소스들은 리트리버와 LLM이 협력하여 사용자의 질의에 대해 관련성 높은 정보를 신속히 제공하는 데 핵심적인 역할을 한다. 기업 환경에서는 이미 각 지식 소스별로 ACL 기반의 접근 정책이 설정되어 있으며, 이러한 관리는 세밀하게 계획되고 운영되고 있으며, 서로 다른 포맷과 인증 체계를 갖는다. 따라서 모든 지식 소스를 단일한 구조로 통합하거나 새로운 접근 제어 정책으로 재설계하는 것은 현실적으로 비용상 매우 어려우며, 보안상 위험도 동반할 수 있다.

그림 3은 RAG 시스템과의 연동을 위해 기존의 지식 소스가 어떻게 구조적으로 개선되어야 하는지를 보여준다. 그림의 상단 부분은 일반적인 형태의 ACL 정책이 적용되는 시스템의 모델이다. RAG와의 연동을 위해서는 지식 소스별로 외부 인터페이스를 구현하여 시스템 간 호환성을 확보해야 한다. 실제 응용 사례에서도 RAG 기반 챗봇 개발 과정에서 데이터 전처리와 인터페이스 설계가 중요한 요소로 다루어졌다[11]. 그림에서 번호는 RAG 시스템과의 상호작용 순서를 보여준다. 제안된 구조는 기존의 데이터 저장소 및 접근 정책을 유지하면서도, 어댑터를 통해 RAG 시스템과의 효과적인 연동을 가능하게 한다.

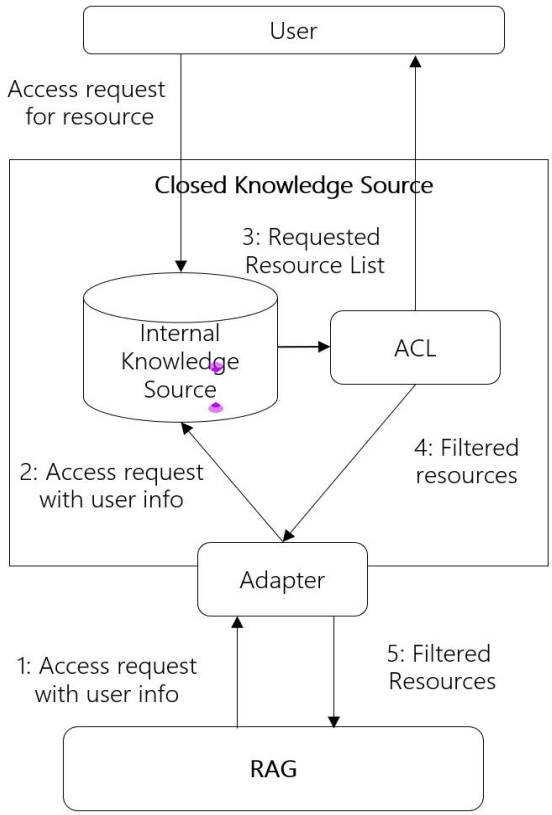

그림 3. RAG 적용을 위한 내부 지식 소스
Fig. 3. Internal knowledge sources for RAG integration

단계 1. RAG 시스템은 사용자 u의 질의 $q_u \in Q$를 어댑터로 요청한다. 이 경우 다수의 정보저장소가 있는 경우 여러 번 요청될 수 있다.

단계 2. 어댑터가 내부 지식 소스에 질의를 입력하면, 내부 지식 소스 전체 정보자원의 집합 $K = \{k_1, k_2, ..., k_n\}$ 의 원소 중에서 관련된 자원을 선택한다. 이 과정을 통해 생성된 요청 정보자원 목록은 $K_u' = retrieve(q_u, K)$ 같이 정의된다:

단계 3. 각 정보자원 $k_i \in K_u'$에 대해 사용자 u의 접근 권한을 확인하고, ACL 정책을 기반으로 허용

된 자원만을 필터링하여 허용 자원 목록을 $K_u^{''} = \{k_i \in K_u^{'} \mid u \in ACL(k_i)\}$로 구성한다.

단계 4. 이렇게 필터링된 정보자원 집합 $K_u^{''}$는 어댑터를 거쳐 RAG에 제공된다.

Ⅳ. 보안성 검증

4.1 사용자 계정 탈취 공격에 대한 ACL 대응

.

공격자는 탈취된 사용자 계정 A_u를 이용하여 민감 데이터 D_s에 접근하려 시도한다. 다시 말해, 공격자는 권한이 없는 상태에서 계정 A_u를 통해 D_s에 접근하려는 위협을 발생시킨다.

접근 허용 여부는 다음과 같은 ACL 정책에 의해 결정된다: 식 (1)에서 보는 바와 같이, P_s는 민감 데이터 D_s에 접근할 수 있는 권한을 가진 사용자 집합이다. 따라서 계정 무결성 즉, 계정이 탈취되지 않음이 보장되는 때에만, ACL은 권한이 없는 주체의 민감 데이터 접근을 차단한다. 즉, ACL 정책은 계정의 권한 정보를 기준으로 접근을 제어하므로, 권한이 없는 계정을 통한 접근은 항상 차단된다. 이는 계정이 정상적으로 유지되고 있는 상황에서 불법 접근을 구조적으로 방지하는 효과가 있다.

$$ACL(A_u, D_s) = \begin{cases} \text{허용} & \text{if } A_u \in P_s \\ \text{거부} & \text{if } A_u \notin P_s \end{cases} \quad (1)$$

4.2 리트리버 질의 조작에 대한 ACL 대응

사용자 A_u가 생성한 리트리버 질의는 식 (2)와 같이 표현된다. 이는 지식 소스 K_b에 대한 요청을 통해 결과 데이터 D를 반환한다. 공격자는 이 질의를 조작하여 권한 없이 민감 데이터 D를 불법적으로 획득하려 시도한다.

$$Q_r(A_u) : K_b \rightarrow D \quad (2)$$

그러나 ACL 정책에 따라 접근 권한은 항상 계정 기준으로 검증된다. 즉, 사용자 A_u가 권한 집합 P_d에 속할 때만 반환 데이터 D에 접근할 수 있다. 따라서 권한이 없는 계정을 이용한 질의 조작은 항상 차단되며, 이는 ACL이 리트리버 질의 조작 공격에 대해서도 효과적으로 방어함을 의미한다.

4.3 프롬프트의 내용 유출 방지

$$P \xrightarrow{expose} D_s \; where \; D_s \subseteq P \quad (3)$$

여기서 P는 ACL의 정책 P에 의하여 필터링된 데이터 집합을 의미하며, D_s는 그중 민감 정보를 나타낸다. 이는 공격자에게 노출될 수 있는 정보 집합이 될 수 있다. 식 (3)에서 보는 바와 같이, 공격자는 프롬프트 내에 포함된 민감 데이터 D_s를 노출할 가능성이 있고, 이는 보안 위협으로 이어질 수 있다. 따라서 프롬프트에 포함된 민감 정보를 보호하기 위해, 폐쇄형 RAG 내부의 프롬프트 구성, 전송, 저장 경로에 대해 암호화, 토큰화, 마스킹 등의 보안 조치가 필요하다.

4.4 지식 소스의 불법 접근

A_k 는 지식 소스 K_b에 접근하려는 공격자이며, D_s는 민감한 데이터이다. 식 (4)에서 보는 바와 같이, 공격자는 권한 없이 지식 소스를 통해 민감 정보를 획득하려 시도한다.

$$A_k : K_b \rightarrow D_s \quad (4)$$

폐쇄형 RAG 시스템은 기존 ACL 정책을 적용하며 운영 중인 지식 소스 K_b를 그대로 활용하므로, 권한 없는 주체가 민감 데이터에 접근하려는 시도는 기존 정책에 의해 자동으로 차단된다. 즉, 별도의 추가 조치 없이도 기존 ACL 정책만으로 불법 접근 위협을 효과적으로 방지할 수 있다.

4.5 문서 저장소의 무단 접근

$$A_k : S_{doc} \rightarrow D_{doc} \quad (5)$$

여기서 A_k는 문서 저장소 S_{doc}에 접근하려는 시도를 나타내며, D_{doc}는 문서 저장소 내의 데이터이다. 식 (5)에서 보는 바와 같이, 공격자는 권한 없이 문서 저장소를 통해 문서 데이터를 획득하려고 시도한다.

문서 저장소 S_{doc}가 이미 운영 중인 ACL 정책에 의해 보호되고 있는 구조이므로, 폐쇄형 RAG 시스템은 별도의 정책 수정 없이 기존 제어 체계를 그대로 계승할 수 있다. 즉, 문서 저장소에 대한 무단 접근 시도는 기존 ACL 정책만으로도 식 (5)에서 정의한 위협을 효과적으로 차단하며, 추가적인 보호 조치 없이도 보안성이 유지된다.

4.6 LLM의 부정확한 응답 생성 방지

공격자는 LLM이 응답을 생성할 때, 자신의 권한을 벗어난 민감 정보 D_s를 참조하게 하여 응답 R에 포함하도록 유도할 수 있다. 식 (6)에서 보는 바와 같이, 이는 권한 없는 사용자가 민감 데이터를 간접적으로 노출하려는 위협을 의미한다.

$$A_u \not\in Ps \ bvt \ D_s \in R \tag{6}$$

본 시스템에서는 사용자 A_u가 입력한 프롬프트에 대해, 리트리버가 내부 문서를 검색하는 과정에서 이미 ACL 정책에 따라 권한 검증이 수행된다. 따라서 LLM이 참조하는 데이터 D는 다음 조건을 만족하는 정보로 제한된다. 즉, 식 (7)에서 보는 바와 같이 LLM은 사용자에게 허용된 문서 범위 내에서만 응답을 생성하게 된다.

$$\forall D_s \in D, A_u \in P_s \tag{7}$$

V. 결론 및 향후 과제

본 논문은 RAG 시스템에 ACL을 적용하여 보안성을 강화하는 구조적 모델을 제안하고, 위협 모델 기반 논리 분석을 통해 그 효과를 검증하였다. 제안된 시스템은 기존 ACL 정책과의 호환성을 유지하면서 다양한 내부 지식 소스와 연동할 수 있으며, 사용자의 질의에 대해 권한 기반 문서 필터링을 통해 무단 접근을 효과적으로 차단하고, 데이터의 기밀성과 무결성을 보장한다. 또한, 데이터 유형별 최적화된 검색 구조와 사전 접근 검증 메커니즘을 통해 보안성과 운영 효율성을 동시에 만족시키는 폐쇄형 RAG 시스템을 구현할 수 있음을 보였다.

향후 연구에서는 RBAC 및 ABAC 기반 정책과의 통합을 통해 보다 유연한 접근 제어 체계를 구축하고, 실제 환경에의 적용 가능성과 운용 성능을 실증적으로 평가할 예정이다. 본 연구는 실제 시스템 구현이나 로그 기반 실험은 수행하지 않았다. 이는 기업 내부의 민감 정보와 ACL 정책이 외부에 공개되기 어렵고, 실제 환경에서의 기술적 통합이 현실적으로 제한되었기 때문이다. 이러한 제약을 고려하여 위협 모델 기반의 논리적 분석으로 대체하였다. 앞으로는 합성 데이터 기반 테스트 베드를 구축하거나 시뮬레이션 환경을 통해, ACL 정책의 응답 차단 효과 및 정보 유출 억제율을 정량적으로 평가할 예정이다. 또한, TLA+ 및 Alloy 도구를 활용한 형식적 검증을 통해 정책 정합성과 구조적 안전성을 분석할 예정이다.

이러한 일련의 연구는 RAG 시스템에서 민감한 데이터를 안전하게 처리할 수 있는 기반 기술을 제공하고, 기업 환경에서 요구되는 실질적인 보안 수준을 충족하는 데 기여할 것으로 기대된다.

References

[1] P. Lewis, B. Oguz, R. Rinott, S. Riedel, and V. Stoyanov, "Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks", Advances in Neural Information Processing Systems (NeurIPS), online, Vol. 33, pp. 9459-9474, Dec. 2020. https://doi.org/10.48550/arXiv.2005.11401.

[2] Z. Zhong, C. Xiong, X. Li, and Z. Wang, "Knowledge-Augmented Generation for Open-Domain Question Answering", Proc. of the Conference on Empirical Methods in Natural Language Processing (EMNLP), Abu Dhabi, pp. 4994-5006, Dec. 2022. https://doi.org/10.18653/v1/2022.emnlp-main.398.

[3] K. Guu, K. Lee, Z. Tung, P. Pasupat, and M. Chang, "REALM: Retrieval-Augmented Language Model Pre-training", Proc. of the 37th International Conference on Machine Learning (ICML), Vienna, Austria, pp. 3929-3938, Jul. 2020. https://doi.org/10.48550/arXiv.2002.08909.

[4] S. Zeng, J. Zhang, P. He, Y. Liu, Y. Xing, H. Xu, J. Ren, Y. Chang, S. Wang, D. Yin, and J. Tang, "The Good and The Bad: Exploring Privacy Issues in Retrieval-Augmented Generation (RAG)", Findings of the Association for Computational Linguistics (ACL), pp. 3456-3467, Jun. 2024. https://doi.org/10.18653/v1/2024.findings-acl.250.

[5] J.-E. Gu and S.-J. Shin, "Design and Implementation of an LLM-Based Interface for a Personalized Agricultural AI Companion System: Based on RAG Model and LangChain Framework", Journal of Internet Broadcasting and Communication (JIIBC), Vol. 24, No. 6, pp. 85-91, Jun. 2024. http://doi.org/10.7236/JIIBC.2024.24.6.85.

[6] E. Bertino and R. Sandhu, "Database Security—Concepts, Approaches, and Challenges", IEEE Transactions on Dependable and Secure Computing, Vol. 2, No. 1, pp. 2-19, Jan. 2005. https://doi.org/10.1109/TDSC.2005.9.

[7] J. Lee, S. Kim, and M. Park, "Security-enhanced Document Retrieval Method for AI-based Chat Systems", Journal of KIIT, Vol. 21, No. 3, pp. 101-110, Jun. 2023. https://doi.org/10.6108/JKIICE.2023.21.3.101.

[8] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models", IEEE Computer, Vol. 29, No. 2, pp. 38-47, Feb. 1996. https://doi.org/10.1109/2.485845.

[9] V. Hu, D. Ferraiolo, D. R. Kuhn, A. Schnitzer, K. R. Sandlin, R. Miller, and K. Scarfone, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations", NIST Special Publication 800-162, National Institute of Standards and Technology, Jan. 2014. https://doi.org/10.6028/NIST.SP.800-162.

[10] M. Valzelli, A. Maurino, M. Palmonari, and B.Spahiu, "A Fine-grained Access Control Model for Knowledge Graphs", Proc. of the 12th International Conference on Knowledge Management and Information Systems (KMIS), online, pp. 595-601, Nov. 2020 https://doi.org/10.5220/0009833505950601.

[11] J.-J. Park, "Development of a Dental Consultation Chatbot Using Retrieval-Augmented Generation (RAG) and Large Language Models", Journal of Internet Broadcasting and Communication (JIIBC), Vol. 24, No. 2, pp. 87-92, Feb. 2024. http://doi.org/10.7236/JIIBC.2024.24.2.87.

저자소개

이 이 섭 (Lee-Sub Lee)

1988년 2월 : 서강대학교 수학과(이학사)
1990년 2월 : 서강대학교 전자계산학과(공학석사)
2004년 9월 : 고려대학교 컴퓨터과(이학박사)
2004년 9월 ~ 현재 : 국립금오공과대학 컴퓨터공학부 교수
관심분야 : 소프트웨어공학, 인공지능, 블록체인