논문 2025-4-9 http://dx.doi.org/10.29056/jsav.2025.12.09

LLM 임베딩 기반 속성 추천 및 SSS 결합 조건은닉 프록시 재암호화 기법

박경엽*, 김현수*, 최창준*, 신동명*†

LLM Embedding-based Attribute Recommendation and SSS Combined Condition Hiding Proxy Re-encryption Technique

Kyung-Yeob Park*, Hyun-Soo Kim*, Chang-Jun Choi*, Dong-Myung Shin*†

요 약

불법 동영상 스트리밍 사이트와 웹툰·출판물 불법 공유 사이트의 확산으로 인해, 국제 공조 수사 과정에서 교환되는 수사 문서와 증거 자료에 대한 안전한 공유 및 접근 제어의 중요성이 더욱 커지고 있다. 본 논문은 명시적인 조직 정책표가 부재한 환경에서 문서 기반 접근 제어를 지원하기 위하여, 대규모 언어 모델(Large Language Model, LLM) 임베딩 기반 속성 추천 기법과 비밀 분산 기법(Secret Sharing Scheme, SSS)을 결합한 조건은닉 프록시 재암호화 기법을 제안한다. 먼저 한글 PDF 수사 문서를 대상으로 문서-속성 라벨 데이터셋을 구축하고, 문서 인코더와 속성 인코더를 통해 두 대상을 동일 임베딩 공간에 투사함으로써, 경험적 정책을 반영한 속성 후보 상위 K개를 추천하는 모델을 설계하였다. 이후 추천된 속성과 문맥 정보를 해시한 조건 스칼라 값을 암호문 지수부에 은닉하고, 서버 비밀값을 Shamir 비밀 분산 기법으로 프록시 계층에 분산함으로써, 반신뢰 환경에서 조건은닉 프록시 재암호화를 수행할 수 있는 프로토콜을 제시하였다. 이를 통해 암호 연산의 안전성뿐만 아니라 운영상의 제약과 위협 모델을 포괄하는 보안·가용성 요구사항 충족 여부를 평가하고 국제 공조 수사 문서 공유 시나리오에서의 적용 가능성을 확인한다.

Abstract

Due to the proliferation of illegal video streaming services and illicit webtoon and publication sharing sites, secure sharing and access control of investigative documents and evidence in international joint investigations have become increasingly critical. This paper proposes a condition-hiding proxy re-encryption scheme that combines a Large Language Model (LLM) embedding-based attribute recommendation method with a Secret Sharing Scheme (SSS) to enable document-centric access control in the absence of explicit organizational policy tables. We construct a document-attribute label dataset from Korean PDF investigation documents, design a model that recommends top-K attributes in a shared embedding space, and embed a hashed condition scalar in the ciphertext exponent while distributing the server secret via Shamir's scheme, thereby evaluating whether the proposed protocol satisfies security and availability requirements under realistic operational constraints and threat models and confirming its applicability to international cooperative investigation scenarios.

한글키워드 : 대규모 언어 모델, 인공지능, 추천 시스템, 암호학, 비밀 분산 기법, 프록시 재암호화

keywords : Large Language Model, Artificial Intelligence, Recommendation System, Cryptography, Secret Sharing Scheme, Proxy Re-Encryption

* 엘에스웨어㈜ 소프트웨어연구소 연구개발본부
† 교신저자: 신동명(email: roland@lsware.co.kr)

접수일자: 2025.11.25. 심사완료: 2025.12.09.
게재확정: 2025.12.20.

www.kci.go.kr

1. 서 론

최근 온라인 환경에서는 불법 동영상 스트리밍 플랫폼과 웹툰/출판물의 불법 공유 사이트가 지속적으로 증가하고 있다. 실제로 국내에서 운영된 PickleTV 및 TV Champ 사례의 경우 2022년부터 2024년까지 넷플릭스, 디즈니플러스 등 주요 OTT 서비스의 영상 32,000편 이상을 무단 유통하여 수 억원 규모의 피해를 입혔다[1]. 이러한 불법 공유 사이트는 정식 서비스에 비해 접근 편의성 등의 이유로 여전히 많은 이용자들이 이용하는 실정이다.

이와 같은 저작권 침해 플랫폼은 서버 인프라를 베트남, 태국 등 해외 지역에 분산하여 운영하는 경향이 있으며, 이로 인해 저작권 단속 및 수사기관 간 국제 공조의 필요성이 증가하고 있다. 이러한 공조 과정에서 교환되는 수사 문서·내부 보고서·증거문서 등은 고도의 민감 정보를 포함하고 있으므로 문서 공유와 접근 제어에 대한 높은 수준의 보안이 필수적이다[2]. 그러나 현행 문서 공유 체계는 이러한 요구를 충족하기에 충분히 정교하지 않다. 실제로 UNODC는 국제 공조 수사 환경에서 사건 관련 정보와 기록의 교환이 필수적이라고 명시하나, 국가/기관 별 접근제어 기준의 차이가 정보 공유 체계의 일관성 확보를 어렵게 한다고 지적한다[3]. 이러한 기준 차이는 현행 시스템이 문서별 접근 정책을 개별적으로 지정하는 방식에 의존하도록 만들고 관리자 수준에서 사용자별·문서별 정책을 수동으로 구성해야 하는 구조로 이어진다. 이 과정에서 정책 누락이나 오류가 발생하기 쉽고 변화하는 수사 환경에 대한 신속한 정책 반영도 어렵다[4]. 이러한 구조적 한계는 복잡한 공조 수사 환경에서 문서 공유의 안전성과 효율성을 낮추는 효과를 가진다. 따라서 문서에서 적절한 접근 속성을 자동으로 도출하고 이를 일관된 방식으로 적용할 수 있는 기술적 기반이 필요하다.

이를 위해 본 논문에서는 대규모 언어 모델(Large Language Model, LLM) 기반의 임베딩 분석을 통해 문서 맥락 정보와 조직 정보를 자동으로 추출하고, 이를 기반으로 접근 제어 정책에 포함될 수 있는 속성(attribute)을 자동 추천하는 기술을 제안한다. 또한, 추천된 속성은 제안하는 조건부 프록시 재암호화(Conditional Proxy Re-Encryption, C-PRE) 구조의 문서 암호화 과정에서 조건으로 반영되어 문서 암호화 시점부터 접근 정책이 강제된다. 이는 설정된 조건을 만족하는 사용자만이 해당 문서를 복호화할 수 있으며 조건을 만족하지 않는 사용자는 암호문을 입수하더라도 복호화가 불가능하게 한다. 또한, 본 연구에서 제안하는 구조는 단일 프록시 서버가 탈취되더라도 재암호화 과정이 악용되지 않도록 프록시가 보유하는 비밀 정보를 비밀 분산 기법(Secret Sharing Scheme, SSS)으로 분할하여 관리하는 구조를 적용하여 프록시는 독립적으로 암호문을 복호하거나 조건을 우회할 수 없으며, 사용자 조각과 서버 조각이 결합될 때에만 재암호화 연산이 가능하다.

2. 관련 연구

2.1 대규모 언어 모델

대규모 언어 모델(LLM)은 대량의 텍스트 코퍼스를 기반으로 사전 학습(pre-training)된 후, 특정 다운스트림 과제에 맞게 미세 조정(fine-tuning)되거나 프롬프트 엔지니어링을 통해 활용되는 범용 자연어 처리 모델을 의미한다[5]. 대표적으로 Transformer 구조를 기반으로 하는 GPT 계열, LLaMA 계열, PaLM 계

www.kci.go.kr

열 모델 등이 있으며, 이들은 문장 생성, 요약, 번역, 질의응답뿐 아니라 문맥 표현 학습을 위한 임베딩 추출에도 널리 활용되고 있다[6].

기존 연구에서는 LLM 또는 대규모 사전학습 언어모델을 이용하여 문서 분류, 민감 정보 탐지, 이상 행위 탐색 등 보안·프라이버시 영역에 적용하려는 시도가 활발히 진행되고 있다[7]. 특히 조직 내부 문서에 대한 정책 추출, 역할 기반/속성 기반 접근제어(RBAC/ABAC) 정책 추천, 감사 로그 분석 등에서 문맥 이해 능력이 우수한 언어모델의 장점이 보고되고 있다[8]. 그러나, 대부분의 연구는 (1) 모델이 생성한 자연어 설명을 사람이 재해석하여 정책으로 반영하거나, (2) 단순 분류 결과를 접근제어 시스템과 별도로 연동하는 수준에 머물러 있어, 암호화 단계에서 접근 조건을 직접 강제하는 구조와는 거리가 있다. 또한, LLM 활용 시에는 환각(hallucination), 편향(bias) 등의 한계와 함께, 민감 문서가 외부 서비스로 전송되는 것에 대한 보안 우려가 존재한다[9].

2.2 비밀 분산 기법

비밀 분산 기법(SSS)은 단일 비밀 값을 여러 조각으로 분할하여, 사전에 정한 임계값(threshold) 이상의 조각이 모였을 때만 원래의 비밀을 복원할 수 있도록 하는 암호 기법이다[10]. 대표적인 Shamir의 비밀분산은 유한체 상의 다항식을 이용하여 (t, n) 스킴을 구성하며, t개 미만의 조각을 획득한 공격자는 정보이론적으로 비밀에 대한 어떠한 추가 정보도 얻을 수 없다. 이러한 특성은 키 에스코로(key escrow), 임계 서명, 분산 키 관리 등 높은 수준의 보안과 가용성이 동시에 요구되는 환경에서 널리 활용되고 있다[11].

프록시 기반 암호 시스템에서도 SSS는 단일 프록시 서버에 민감한 키 정보를 집중시키지 않기 위한 수단으로 사용될 수 있다. 기존 연구들에서는 프록시 서버를 다수의 노드로 분할하여 각 노드에 키 조각을 분산 저장하고, 임계 개수 이상의 노드가 협력할 때에만 재암호화를 수행하도록 설계함으로써, 일부 노드가 탈취되더라도 전체 시스템의 비밀이 노출되지 않도록 한다. 그러나 많은 경우 SSS는 키 백업 또는 장애 대응 관점에서 활용되는 수준이며, 프록시 재암호화 과정 전체에 걸쳐 키 조각의 생성·조합·폐기를 정교하게 설계한 연구는 상대적으로 제한적이다[12].

2.3 조건부 프록시 재암호화

프록시 재암호화(PRE)는 제3자인 프록시가 평문을 알지 못한 채, 특정 사용자의 공개키로 암호화된 암호문을 다른 사용자의 공개키 기반 암호문으로 변환할 수 있도록 하는 공개키 암호 기법이다[13]. 일반적인 PRE 스킴에서는 위임자(delegator), 수신자(delegatee), 프록시(proxy)가 존재하며, 위임자가 프록시에게 재암호화 키(re-encryption key)를 제공하면, 프록시는 이를 이용해 암호문을 변환할 수 있다. PRE는 클라우드 스토리지, 이메일 위임, 콘텐츠 배포 등 다양한 환경에서 동적 권한 위임 기능을 제공하는 핵심 기술로 활용되어 왔다.

조건부 프록시 재암호화(Conditional Proxy Re-encryption)는 여기에 속성(attribute), 시간, 문맥(context) 등 특정 조건을 추가하여, 조건을 만족하는 경우에만 재암호화가 가능하도록 확장한 구조이다. 일부 연구에서는 속성 기반 암호(Attribute-based Encryption, ABE)와 결합하여, 암호문에 정책을 포함하거나 사용자 속성에 기반한 미세 접근 제어를 실현하고자 하였다[14]. 그러나, 많은 스킴에서 조건 값이 암호문 또는 재암호화 키에 평문 또는 준평문 형태로 포함되어, 프록시나 제3자가 조건

www.kci.go.kr

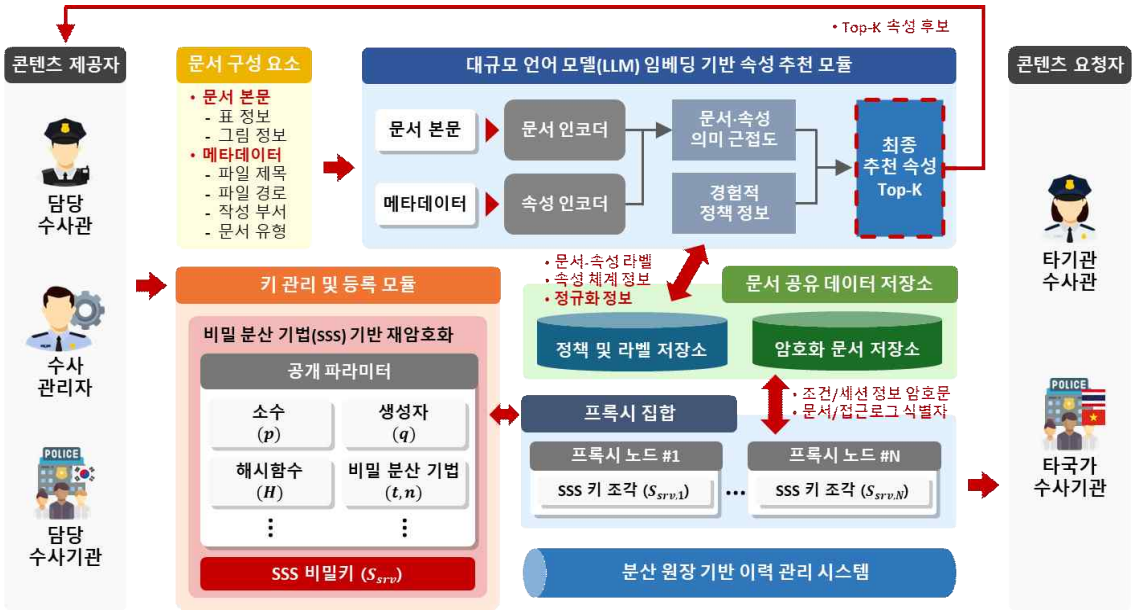

그림 1. 제안 시스템 구성도
Fig 1. Proposed System Architecture

구조를 추론할 수 있는 한계가 존재한다[15]. 이에 대한 보완으로, 조건의 구체적인 값을 외부에서 직접적으로 파악할 수 없도록 하는 조건은닉(Condition Hiding) 프록시 재암호화 스킴이 제안되었으나, 여전히 (1) 조건 설정을 관리자가 수동으로 수행하거나, (2) 서버를 완전 신뢰 가능한 주체로 가정하는 경우가 많다[16]. 한글 문서 처리 기술이 문서 분류나 정보 추출과 같은 독립된 분석 기능에 중점을 두는 것과 달리 본 연구는 문서 분석 결과를 암호화 기반 접근제어의 조건으로 직접 활용하는 통합 구조를 제안한다. 이러한 구조는 문서 임베딩에서 도출된 속성을 재암호화 조건으로 결합하여 문서 분석 단계와 암호화 단계가 연동되는 일관된 정책 강제 체계를 제공한다.

3. 시스템 설계

본 장에서는 제안 기법이 적용되는 국제 공조 수사 문서 공유 환경을 대상으로, 시스템을 구성하는 주요 요소와 이들이 상호 작용하는 구조를 정의한다. 또한 도입 초기 단계에서 고려해야 할 보안·운영상 요구사항을 체계적으로 정리함으로써 이후 4장에서 제시하는 구체적 알고리즘 및 프로토콜 설계의 전제 조건을 명확히 한다. 기존

3.1 시스템 설계 구성요소

제안 시스템은 수사기관 간 문서 공유 및 접근 제어를 지원하기 위해 그림 1과 같은 구성요소로 이루어진다.

첫째, 콘텐츠 제공자는 저작권 침해 수사 보고서, 증거 자료 정리 문서 등 민감 문서를 생성·보유한 수사관 또는 담당자를 의미하며, 로컬 클라이언트 또는 내부 포털을 통해 문서를 업로드하고 LLM 기반 속성 추천 결과를 검토·선택한 후

www.kci.go.kr

암호화 및 조건 설정을 요청한다. 콘텐츠 요청자는 국제 공조 또는 내부 협업 과정에서 해당 문서에 접근해야 하는 타 기관·타 부서 수사관으로, 자신의 속성(소속, 부서, 계급/직위, 직무, 사건 분야 등)에 기반한 인증을 수행한 뒤 시스템에 문서 접근 요청을 전달한다. 두 유형의 사용자는 동일한 보안 정책 하에서 각 역할(생성·공유 vs. 조회·활용)을 수행하는 주체로 정의된다.

둘째, LLM 임베딩 기반 속성 추천 모듈은 문서 인코더와 속성 인코더를 포함하며, 문서 본문과 메타데이터를 입력으로 받아 공통 임베딩 공간에서 후보 속성들에 대한 의미 근접도와 경험적 정책을 결합한 최종 점수를 계산한다. 그 결과로 Top-K 속성 후보와 함께 근거 문장/표를 반환하여, 사용자가 직관적으로 추천 결과를 검토·수정할 수 있도록 한다. 추천 모듈은 온프레미스 환경에서 동작하거나, 문서 내용이 외부로 유출되지 않도록 보호된 실행 환경에서 운영된다.

셋째, 문서 공유 데이터 저장소에서의 정책 및 라벨 저장소(Empirical Policy Repository)는 문서-속성 라벨, 조직별 경험적 정책, 속성 체계 및 정규화 정보를 저장·관리하며, 속성 추천 모듈의 학습·추론 과정에서 참조될 뿐 아니라 운영 중 축적되는 사용자 선택 결과를 반영하여 정책을 점진적으로 보정하는 역할을 수행한다. 암호화 문서 저장소(Encrypted Document Repository)는 조건·세션 정보가 포함된 암호문과 cond_id, 문서 식별자, 접근 로그 식별자 등을 저장하며, 평문은 저장하지 않는다. 이를 통해 정책 정보와 암호문이 분리된 형태로 관리되면서도, 상호 참조를 통해 세밀한 접근 제어를 구현할 수 있다.

넷째, 프록시 집합은 여러 개의 프록시 노드로 구성되며, 서버 측 비밀값을 Shamir SSS로 분할한 조각을 각각 보유한다. 이는 초기 세팅 단계에서 분배된 조각을 이용하여 재암호화, 조건 변경, 복호화 보조 연산에 필요한 지수 연산을 수행하지만, 어떤 단일 노드도 완전한 키를 구성할 수 없다. 또한, 프록시 집합은 재암호화·조건 변경 요청에 대한 감사 로그를 별도로 기록하여, 오용 여부를 사후 분석할 수 있도록 한다.

다섯째, 키 관리 및 등록 모듈은 사용자 등록, 속성 인증, 사용자 비밀 조각 생성, 공개키 계산 및 등록을 담당한다. 사용자는 자신의 단말에서 사용자 비밀 조각을 생성하고, 서버는 SSS로 분할된 서버 측 비밀 조각을 프록시 노드에 배포한다. 이를 통해 시스템 데이터베이스에는 완성된 형태의 개인키가 저장되지 않으며, 공개키만이 재암호화 과정에서 사용된다.

여섯째, 분산 원장 기반 이력 관리 시스템은 속성 추천 결과 선택, 조건 변경, 재암호화 수행, 복호화 성공·실패 등의 이벤트를 시간순으로 기록한다. 이는 보안 사고 발생 시 원인 분석과 책임 추적을 가능하게 할 뿐 아니라, 장기적으로는 운영 데이터를 기반으로 정책과 파라미터를 튜닝하는 데 활용될 수 있다.

이러한 구성요소는 '문서 업로드 → 속성 추천 및 검토 → 조건 포함 암호화 → 프록시 저장 및 재암호화 → 요청자 복호화'의 흐름으로 상호 연동되며, 각 단계에서 최소 권한 원칙과 반신뢰 가정을 만족하도록 설계된다.

3.2 시스템 요구사항

제안 시스템은 국제 공조 수사 환경에서의 실사용을 목표로 하므로, 단순 암호 연산의 안전성뿐 아니라 운영상의 제약과 위협 모델을 포괄하는 보안·가용성 요구사항을 충족해야 한다. 본 절에서는 이를 기밀성, 가용성, 반신뢰, 데이터 정합성 및 무결성, 조건 검증 강제성의 다섯 관점으로 정리한다.

3.2.1 기밀성(Confidentiality)

시스템은 문서 라이프사이클 전 구간에서 평문 데이터가 문서 소유자 외의 주체에게 노출되

www.kci.go.kr

지 않도록 보장해야 한다. 구체적으로, (1) 문서가 암호화되기 전 단계는 로컬 클라이언트 또는 보호된 실행 환경 내에서만 처리되며, (2) 저장소 및 프록시 집합에는 평문이 아닌 암호문과 메타데이터만 저장된다. 프록시는 재암호화 과정에서 평문에 접근하지 않고 지수 연산만 수행하도록 설계되며, 조건 값 역시 스칼라 형태로 해시·은닉되어 외부에서 조건 구조를 추론할 수 없다. 또한, LLM 임베딩 기반 속성 추천 단계에서도 문서 내용과 임베딩 벡터는 시스템 경계 밖으로 전송되지 않도록 하고, 모델 파라미터 학습 시에는 익명화·비식별화·내부 데이터 전용 환경 등을 통해 2차 유출을 방지해야 한다.

3.2.2 가용성(Availability)

시스템은 수사 환경의 특성상 긴급한 문서 공유 요청이 빈번히 발생함을 고려하여, 언제든 속성 추천, 조건 변경, 재암호화 요청을 처리할 수 있어야 한다. 이를 위해 프록시 집합과 암호화 문서 저장소는 장애 조치(failover) 및 수평 확장 구조를 지원해야 하며, 특정 노드 장애 시에도 임계값(t) 이상의 프록시 노드가 유지되는 한 재암호화 서비스가 중단되지 않아야 한다. 또한, 콘텐츠 제공자가 오프라인 상태이더라도, 사전에 설정된 조건과 키 구조만으로 콘텐츠 요청자의 접근 요청을 처리할 수 있도록 설계하여, 업무 연속성을 보장한다. LLM 기반 속성 추천 모듈 역시 캐시, 배치 처리, 우선순위 큐 등을 활용하여 대량 문서 처리 상황에서도 응답 지연을 최소화해야 한다.

3.2.3 반신뢰(Semi-trust)

프록시 노드는 시스템 운영상 필수적인 중개자이지만, 완전히 신뢰할 수 있는 주체로 가정하지 않는다. 프록시는 정해진 프로토콜을 정직하게 수행한다고 가정하되(honest-but-curious), 저장된 암호문과 키 관련 정보를 분석하여 평문이나 조건, 사용자 속성을 추론하려 할 수 있는 주체로 간주한다. 따라서 (1) 프록시는 자체적으로 어떠한 복호 연산도 수행할 수 없어야 하며, (2) 단일 프록시 노드의 탈취만으로는 서버 측 비밀값을 복구할 수 없어야 한다. 이를 위해 서버 비밀값을 SSS로 분할하여 각 노드에 조각 형태로 분산 저장하고, 재암호화·조건 변경·복호화 보조 연산 시에도 조각 상태에서만 연산이 수행되도록 한다. 또한, 프록시와 사용자가 공모하더라도 임계값 t 미만의 조각으로는 유의미한 정보를 복구할 수 없도록 유한체 기반 정보 이론적 안전성을 유지해야 한다.

3.2.4 데이터 정합성 및 무결성(Integrity)

암호문의 구성요소인 C_1 , C_2 또는 cond_id가 전송 중 혹은 저장 중 변조될 경우, 어떤 사용자도 정상적인 복호화를 수행할 수 없어야 하며, 가능하다면 변조 시도를 탐지할 수 있어야 한다. 이를 위해 암호 시스템은 암호문과 메타데이터에 대해 메시지 인증 코드(MAC) 또는 디지털 서명과 같은 무결성 보호 메커니즘을 결합해야 한다. 또한, 조건 변경 및 재암호화 단계에서 생성되는 새로운 암호문에 대해서도 동일한 무결성 검증 절차를 적용하여, 프록시나 네트워크 공격자가 임의의 값을 삽입하거나 기존 암호문을 재활용(replay)하더라도 복호화가 실패하도록 설계해야 한다. 로그 저장소에는 각 연산의 입력·출력 식별자 및 시각 정보를 기록하여, 이상 행위 탐지 및 사후 감사가 가능하도록 한다.

3.2.5 조건 검증 강제성(Attribute-Condition Enforcement)

시스템은 속성 기반 조건이 암호화 단계에서부터 강제되도록 보장해야 하며, 조건을 만족하지 않는 사용자는 암호문을 획득하더라도

www.kci.go.kr

복호화에 실패해야 한다. 제안 기법에서는 문서 속성 v와 문맥 정보 ctx로부터 조건 스칼라 값 δ를 계산하여 지수부에 은닉하고, 사용자 공개키와 결합된 형태의 암호문을 생성한다. 이때 사용자 측 속성과 시스템에 등록된 속성 정보가 불일치하면, 복호화를 위해 필요한 지수 구성요소를 올바르게 재구성할 수 없으므로 평문 복원에 실패한다. 중요한 점은, 조건 불일치 시에도 공격자에게 추가적인 측면 정보(side information)가 노출되지 않아야 한다는 것이다. 즉, 실패 여부 외에 조건 구조나 사용자 속성이 어떤 부분에서 불일치했는지에 대한 단서는 제공하지 않아야 한다. 이를 통해 조건은닉(Condition Hiding) 특성을 유지하면서도, 문서 단위·업무 라인 단위의 세밀한 접근 제어 정책을 암호 시스템 내부에서 직접 강제하는 것이 본 시스템의 핵심 목표이다.

4. 제안 기술

4.1 데이터셋 구성

제안 기술에서 활용하는 데이터셋은 한글 PDF 문서를 기반으로 문서 단서, 문서별 속성 라벨(키-쌍 집합)을 포함한다. 이는 명시적 조직 정책표가 제공되지 않는 환경을 전제로 하며, 문서 - 속성 간의 공동 출현 패턴을 경험적 정책(empirical policy)으로 정의하여 학습 및 평가에 활용한다. 본 연구에서는 기밀성이 요구되는 실제 수사보고서를 직접 활용하기 어려운 점을 고려하여 초기 실험 단계에서는 공개 PDF 데이터셋인 FinePDFs를 활용한다[17]. FinePDFs는 다양한 도메인의 문서로 구성된 공개 데이터셋으로 데이터 구성과 품질이 투명하게 공개되어 있어 데이터의 객관성을 보장할 수 있다. 본 연구에서는 해당 데이터셋을 이용하여 문서 임베딩 및 속성 추천 과정의 동작을 검토하였으며 향후 실제 수사보고서로의 확장을 위해 도메인 특화 어휘와 구조적 패턴을 반영한 추가 실험을 수행할 계획이다. 데이터셋은 아래와 같이 구성된다.

4.1.1 데이터 표현 및 레코드 구조

각 문서 레코드는 아래와 같은 요소로 구성된다.

- **문서 내용:** PDF에서 획득한 본문과 표 정보로 의미 파악에 불필요한 반복 머리말, 쪽번호, 워터마크 등은 최소한으로 정리하였으며 부서명·관할·보안 표기·기관명·사건 분야 등 접근 판단에 유의미한 표현은 그대로 보존한다. 또한 표 형태의 내용은 제목, 열 이름, 핵심 셀을 문장형 단서로 변환하여 문맥을 보완한다.
- **메타데이터:** 문서의 정체성과 맥락이 포함되는 기본 정보로써 파일 제목, 파일 경로, 작성 부서, 문서 유형 등으로 구성된다.
- **속성 라벨:** 특정 문서에 접근 가능한 속성의 키-값 집합(e.g., 소속=경찰청, 부서=사이버범죄)으로 모든 키에 반드시 값이 포함되는 것은 아니며, 문서 성격에 따라 일부 값이 생략될 수 있다.

이러한 표현 방식은 문서의 실제 맥락을 보존하면서도 이후 과정에서 추천 결과를 검토하고 설명하기 위한 근거 확보에 활용할 수 있다.

4.1.2 라벨 구성 및 경험적 정책 활용

라벨은 문서 접근이 실제로 허용된 속성을 중심으로 정리하며, 공식 정책표가 부재한 환경을 전제로 데이터에 나타난 공통적인 조합을 경험적으로 신뢰도가 높은 규칙으로 간주한다. 예를 들어, 특정 부서의 문서에서 속성 조합(e.g., 소속=경찰청, 부서=사이버범죄)이 일관되게 나타난다면, 이는 해당 부서 문서의 표준 접근 속성으로 해석한다. 이러한 해석은 라벨 품질을 검증하는 기준선 및 추

www.kci.go.kr

천 결과의 정렬 기준으로 활용되어 데이터 내에서 반복적으로 등장하는 속성 조합은 정책적 일관성이 높은 것으로 간주하고 상위에 배치되며, 이례적이거나 문맥상 불일치한 조합은 상대적으로 낮은 우선순위를 부여한다. 모델은 이러한 패턴을 통해 명시적 규칙 없이도 정책의 경향성을 학습한다.

4.1.3 속성 체계 및 용어 정규화

실제 수사 및 국제 공조 업무에서는 기관·부서·직무·관할·사건유형 등 업무 단위가 명확히 구분되어 운영되며 문서와 기록의 접근 주체 또한 이러한 조직적 역할 분리에 따라 달라진다. 따라서 문서 접근 정책을 구성하는 속성 체계는 실무 환경에서 반복적으로 등장하는 역할·기관·관할·사건 관련 단서를 중심으로 정의될 필요가 있다. 본 연구의 속성 체계는 이러한 실제 업무 구조에서 관찰되는 공통적인 구분 기준을 반영하여 설계하였다. 해당 속성 체계는 표 1과 같이 정의하며, 각 키의 값은 조직 내에서 실제로 사용하는 표기를 기준으로 “사이버수사과/사이버팀”처럼 표기가 다양한 항목은 하나의 표준 용어로 정규화한다. 이러한 용어 정규화는 데이터의 일관성을 높이며 추천 결과의 해석을 용이하게 한다.

표 1. 속성 체계 목록
Table 1. Attribute Scheme List

구 분	설 명	예 시
국가	- 수사 주체 기관이 속한 국가	KR, JP 등
소속(기관)	- 수사 담당 주요 기관명	경찰청, 문화체육관광부 등
부서	- 사건을 담당하는 실무 부서	사이버범죄 등
계급/직위	- 담당자의 직급 또는 책임 수준	경위, 경감 등
직무(역할)	- 문서 처리 및 분석 담당 역할	수사관, 조사관 등
근무지역	- 사건 관할 또는 기관 소재지	서울, 경기 등
사건 분야	- 수사 대상 사건 유형	저작권 침해, 불법복제 등
보안 등급	- 문서의 기밀성 수준	제한, 기밀 등

4.2 LLM 임베딩 벡터 기반 속성 정보 추천

본 절에서는 문서 파일을 입력으로 하여 해당 문서에 접근할 수 있는 수사관의 속성 정보 후보 상위 K개를 추천하는 방법을 제안한다. 제안 기술에서는 문서와 속성을 동일 임베딩 공간에 투사해 의미 근접도를 계산하고, 데이터에서 반복되는 경험적 정책(문서 계열별 반복 및 일관성, 문맥 합치 등)을 가중하여 정밀도를 우선으로 재정렬하여 추천 결과에 간결한 근거를 함께 제시하도록 설계하였다.

제안 기술은 문서 f의 기본 메타데이터를 입력받아 d차원 실수 벡터 공간의 문서 임베딩 $z_f \in R^d$를 산출하는 문서 인코더 E_f와 속성 a를 속성 임베딩 E_a로 변환하는 속성 인코더 E_a로 구성된다. 문서-속성 의미 근접도는 후보 생성 단계에서 1차 점수로 사용되며 문서 임베딩 벡터와 속성 임베딩 벡터의 내적을 통해 계산된다. 수식은 다음과 같다.

$$s_{sim}(f,a) = z_f^T z_a$$

본 모델은 문서 f에 대한 정답(positive) 속성 a^+와 유사도를 높이고 다른 속성 집합 N과의 유사도를 낮출 수 있도록 대비 학습을 수행한다. 학습 과정에서 온도(temperature)값 r을 적용하여 정답 속성과 다른 속성 간 점수 차이를 더욱 선명하게 반영한다. 해당 수식은 아래와 같이 표현된다.

$$L(f,a^{+}) = -\log\frac{\exp(s_{sim}(f,a^+/r))}{\exp(s_{sim}(f,a^+/r)) + \sum_{a\in N}\exp(s_{sim}(f,a/r))}$$

위 수식의 분자는 정답 쌍의 유사도를 지수화한 값이며, 분모는 정답 쌍과 다른 속성 집합 N의 지수값의 합으로 구성된다. 이러한 확률값을 극대화

www.kci.go.kr

(또는 손실 값을 최소화)함으로써 모델은 정답 속성이 가장 높은 점수를 가지도록 학습한다.

최종 추론 단계에서는 문서-속성 의미 근접도인 $s_{sim}(f,a)$와 업무 라인 L(경로/작성부서 등으로 추정)에서 키와 값 쌍의 출현 비율을 정규화한 값인 $\pi_{freq}(a|L)$, 본문이나 표에서 추출한 단서와 속성 a를 맵핑하여 일치 점수를 계산한 $\pi_{ctx}(a|f)$, 후보 속성 a가 문서 f와 일치하지 않을수록 커지는 감점 신호인 $\pi_{mis}(a|f)$를 이용하여 아래 수식과 같이 $s_{final}(f,a)$를 계산한다.

$$s_{final}(f,a) = \alpha \cdot s_{sim}(f,a) + \beta \cdot \pi_{freq}(a|L) + \gamma \cdot \pi_{ctx}(a|f) - \delta \cdot \pi_{mis}(a|f)$$

최종 점수는 수식처럼 기본 근접도에 경험적 정책을 선형 결합하여 정의되며 Top-K는 s_{final}을 기준으로 내림차순 정렬하고 동일 키가 상위에 과도하게 중복되지 않도록 키 별 최대 개수 제약(e.g., 보안등급은 최대 1개)을 적용한다. 최종적으로 본 모델은 점수와 함께 각 선택 항목에 대하여 점수에 기여한 상위 단서(문장/표 등) 및 업무 라인 정보 L을 짧게 요약해 근거로 첨부한다. 콘텐츠 제공자는 추천된 Top-K 속성 후보 중 적합한 항목을 검토·선택하고, 선택된 속성은 다음 단계인 속성 기반 프록시 재암호화 과정의 입력값으로 활용된다.

4.3 SSS 기반 조건부 프록시 재암호화

본 절에서는 이전 단계에서 콘텐츠 제공자가 선택한 속성 정보를 조건값으로 사용하여 콘텐츠 요청자에게 데이터를 공유할 수 있도록 하는 조건부 프록시 재암호화 과정을 기술한다. 조건부 프록시 재암호화는 초기 세팅 단계, 키 생성 단계, 암호화 단계, 단순 조건 변경 단계, 재암호화 단계, 복호화 단계로 구성된다.

4.3.1 초기 세팅 단계

암호 시스템은 소수 p와 생성자 g에 의해 정의되는 유한군 $G=\langle g\rangle \subseteq Z_p^*$를 사용하며, g의 차수 q는 소수로써 $q|(p-1)$을 만족한다. 암호 시스템은 조건으로 사용되는 속성값을 정수 스칼라로 변환하도록 해시함수 $H_{attr}:\{0,1\}^* \rightarrow Z_q$을 설정한다. 시스템은 프록시 측 복호 지수로 이용할 비밀 조각인 $s_{srv} \in Z_q$를 생성하고, 이를 아래의 다항식을 통해 shamir (t,n) 비밀분산 기법으로 분할하여 $\{s_{srv,1},\ldots,s_{srv,n}\}$ 형태로 각 프록시 노드에 배포한다. 계수 a_i를 유한체 Z_q에서 무작위로 선택하여 다항식을 구성함에 따라 상수항 s_{srv}의 값을 다항식 내에 안전하게 은닉할 수 있다.

$$share_i = f(i) = s_{srv} + a_1 i + a_2 i^2 + \cdots + a_{t-1} i^{t-1} \pmod q$$

계산이 완료된 (p,q,g,H_{attr},t,n)은 공개 파라미터로써 프록시 재암호화 과정 전체에서 활용한다.

4.3.2 키 생성 단계

해당 암호 시스템에서 모든 사용자(참여자)는 동일한 키 구조를 가진다. 먼저 시스템은 초기 세팅 단계에서 정의된 공통 서버 비밀값 $s_{srv} \in Z_q$를 이미 보유하고 있으며, 이는 shamir (t,n) 비밀분산을 통해 각 프록시 노드에 $(i,f(i))$ 형태로 배포되어 있다. 개별 사용자 U는 단말에서 자신의 사용자 비밀 조각 $s_{usr,u} \in Z_q$를 독립적으로 생성한다. 이때 사용자 U의 개인키는 sk_U로 표현되며 수식은 아래와 같다.

$$sk_U = s_{srv} + s_{usr,U} \pmod q$$

이러한 개인키는 프록시와 사용자 측이 각각 고유 조각만 보유하고 있으므로 완전한 개인키

www.kci.go.kr

값은 어떤 단일 주체에도 노출되지 않는다. 사용자 공개키는 두 키 조각에 대응하는 지수형 공개값을 곱하여 합성한다. 이 과정은 프록시가 보유한 서버 측 공개값과 사용자가 계산한 사용자 측 공개값을 이용하여 이루어지며 이를 수식으로 나타내면 아래와 같다.

$$PK_U = PK_{srv} \cdot PK_{usr,U} = g^{s_{srv}} \cdot g^{s_{usr,U}} \equiv g^{s_{srv}+s_{usr,U}} \pmod{p}$$

생성된 공개키는 프록시 서버에 등록되며, 이러한 구성을 통해 시스템에는 완성된 형태의 사용자 공개키만이 저장되고, 대응하는 개인키는 항상 n개로 분할된 서버 조각과 사용자 조각의 상태로 존재한다. 이후 수행되는 모든 암호 관련 연산에서 서버측 비밀 조각 s_{srv}는 n개의 분할 조각 형태로 유지되며, 각 단계의 연산 시 조합 과정을 통해 필요한 서버 측 키 성분으로 활용된다.

4.3.3 암호화 단계

본 단계에서 콘텐츠 제공자 A는 4.2절에서 선택한 속성 σ와 문서 정보 ctx(e.g., 문서 생성 일자, 문서 ID)를 해시화하여 조건 스칼라 값 θ를 도출한다. 해당 조건값은 복호화 시점에서 이용자의 속성과 문서 조건의 일치 여부를 확인하는 요소로 활용되며, 단순 비교 문자열이 아닌 속성과 문서 맥락을 포함하는 수치화된 형태로 조건을 은닉할 수 있도록 설계되었다.

$$\theta = H_{attr}(\sigma \parallel ctx) \bmod q$$

조건 스칼라 값 계산 이후 같은 조건값이라도 매번 새로운 암호문을 생성할 수 있도록 일회용 난수 $r \in Z_q$를 선택하고 콘텐츠 제공자 A는 난수값과 생성자 g를 사용해 아래와 같이 세션값을 계산한다.

$$C_1 = g^r \bmod p$$

C_1은 복호화 과정에서 조건 및 키 정보가 지수 형태로 재구성하는데 활용되며, 일회용 난수 r로부터 계산되므로 동일한 속성 정보 σ와 문맥 정보 ctx로 θ가 동일하더라도 암호문을 랜덤화할 수 있다. 이를 통해 조건 추론이 불가능해지도록 조건을 은닉할 수 있다.

평문 M은 콘텐츠 제공자 A의 공개키에 조건 스칼라 θ와 난수 r이 곱해진 조건·세션 결합 지수값과 결합하여 암호화된다. 이는 아래 수식과 같이 표현되며 조건 정보가 지수부에 은닉된 형태로 포함되므로 조건 값은 평문 형태로 노출되지 않는다.

$$C_2 = M \cdot PK_A^{\theta \cdot r} \bmod p$$

최종 암호문 C는 앞서 계산된 C_1과 C_2, 그리고 검증 시 참조할 수 있는 조건 식별자 cond_id와 함께 아래의 형태로 구성된다. 이러한 과정은 프록시나 제3자 조건 검증없이 평문을 복구할 수 없게 한다.

$$C = (C_1, C_2, cond\_id)$$

4.3.4 조건 변경 단계

본 단계는 원본 콘텐츠 M이 이미 콘텐츠 제공자 A의 공개키와 특정 조건 스칼라 θ로 암호화되어 프록시에 저장되어있는 상황을 가정한다. 해당 단계는 콘텐츠 제공자 A가 속성 조건을 σ_{old}에서 σ_{new}로 변경하여도 평문을 복호화하지 않고 암호문 내부의 조건 지수부만 갱신할 수 있음을 증명한다.

먼저 콘텐츠 제공자 A는 새로운 조건의 σ_{new}를 통해 θ_{new}를 계산하고 두 조건 스칼라 간의 변화량인 δ를 계산한 후 프록시에게 해당 값을 전달한다.

$$\delta = \theta_{new} - \theta_{old} \bmod q$$

www.kci.go.kr

콘텐츠 제공자 A와 프록시는 각각 비밀 조건인 s_{srv}, $s_{usr,A}$ 및 조건 스칼라 변화값 δ를 이용하여 $F_{srv,\delta}$와 $F_{usr,\delta}$를 계산한다. 이후 $F_{usr,\delta}$는 프록시 서버로 전달되며, 프록시 서버는 해당 값들을 곱해 F_{δ}값을 산출한다.

$$F_{srv,\delta} \equiv C_1^{\delta \cdot s_{srv}},\ F_{usr,\delta} \equiv C_1^{\delta \cdot s_{usr,A}} \bmod p$$

$$F_{\delta} \equiv F_{srv,\delta} \cdot F_{usr,\delta} \equiv C_1^{\delta(s_{srv}+s_{usr,A})} \equiv g^{r\delta(s_{srv}+s_{usr,A})} \equiv PK_A^{\delta r} \bmod p$$

계산된 F_{δ}은 기존 암호문인 C_2와 곱해져 기존 조건 스칼라값 θ_{old}에 대응하는 지수항이 제거되고, 대신 새로운 조건 스칼라 θ_{new}가 반영된 $C_2^{'}$이 생성된다. 이 과정에서 프록시는 θ_{old}, θ_{new}, r 등 어떠한 비밀값도 알 수 없다. 이를 수식으로 나타내면 아래와 같다.

$$C_2^{'} \equiv C_2 \cdot F_{\delta} \equiv (M \cdot PK_A^{\theta_{old} \cdot r}) \bullet PK_A^{\delta \cdot r} \equiv M \cdot PK_A^{(\theta_{old}+\delta)r} \equiv M \cdot PK_A^{(\theta_{old}+(\theta_{new}-\theta_{old}))r} \equiv M \cdot PK_A^{\theta_{new} \cdot r} \bmod p$$

4.3.5 재암호화 단계

해당 단계에서 콘텐츠 제공자 A의 공개키 기반 암호문 C_2는 평문 M 및 조건/세션 정보를 노출하지 않고 콘텐츠 요청자 B의 공개키 기반 암호문 $C_2^{''}$으로 변경된다. 이때, 프록시는 θ와 r값을 알 수 없으며, 각 단말에서 제공하는 지수 값들만 곱하여 암호문을 변환한다. 이 과정에서 콘텐츠 제공자 A는 자신의 비밀 조각을 상쇄하는 보정 값 F_A^{-}를 계산하고, 콘텐츠 요청자 B는 자신의 비밀 조각을 포함시키는 보정값 F_B^{+}을 계산하여 각각 프록시에 전달한다.

$$F_A^{-} \equiv (C_1^{\theta \cdot s_{usr,A}})^{-1},\ F_B^{+} \equiv C_1^{\theta \cdot s_{usr,B}} \bmod p$$

프록시는 두 보정값 F_A^{-}와 F_B^{+}를 사용해 암호문 C_2를 재암호화 시킬 수 있는 재암호화 파라미터 F_{re}를 계산한다.

$$F_{re} \equiv F_B^{+} \cdot F_A^{-} \equiv C_1^{\theta(s_{usr,B}-s_{usr,A})} \equiv g^{\theta r(s_{usr,B}-s_{usr,A})} \bmod p$$

프록시가 계산한 재암호화 파라미터 F_{re}는 기존 암호문 C_2와 곱해져 콘텐츠 요청자 B가 복호화할 수 있는 형태의 재암호화된 암호문 $C_2^{''}$을 생성한다. 이후 프록시는 이 암호문을 포함하는 최종 암호문 C를 콘텐츠 요청자 B에게 전송한다. 해당 과정을 수식으로 나타내면 아래와 같다.

$$C_2^{''} \equiv C_2 \cdot F_{re} \equiv (M \cdot g^{\theta r(s_{srv}+s_{usr,A})}) \cdot g^{\theta r(s_{usr,B}-s_{usr,A})} \equiv M \cdot g^{\theta r(s_{srv}+s_{usr,B})} \equiv M \cdot PK_B^{\theta \cdot r} \bmod p$$

4.3.6 복호화 단계

해당 단계에서 콘텐츠 요청자 B는 자신의 공개키 PK_B만 알고 있는 상황으로 조건·세션 결합 지수 값 $\theta \cdot r$을 알 수 없다. 이에 대응할 수 있는 키 성분을 얻기 위해 암호문 구성요소 C_1과 자신의 비밀 조각 $s_{usr,B}$를 이용하여 복호화에 필요한 구성요소 D_{usr}을 계산한다. 또한, 프록시에 서버 측 비밀 조각 s_{srv}과 C_1을 이용한 D_{srv}를 계산하도록 요청한다.

$$D_{srv} \equiv C_1^{\theta \cdot s_{srv}},\ D_{usr} \equiv C_1^{\theta \cdot s_{usr,B}} \bmod p$$

두 구성요소 D_{srv}와 D_{usr}의 곱은 콘텐츠 요청자 B의 공개키에 조건·세션 결합 지수 값을 지수화한 값과 같으며, 따라서 콘텐츠 요청자 B는 해당 값의 역원을 계산한 후 재암호화된 암호문 $C_2^{''}$과 곱하면 원본 콘텐츠 M을 획득할 수 있다.

www.kci.go.kr

$$D \equiv D_{srv} \cdot D_{usr} \equiv C_1^{\theta(s_{srv}+s_{usr,B})} \equiv PK_B^{\theta \cdot r} \mod p$$

$$M \equiv C_2'' \cdot D^{-1} \equiv M \cdot PK_B^{\theta \cdot r} \cdot (PK_B^{\theta \cdot r})^{-1} \equiv M \mod p$$

5. 제안 기술 평가

본 장에서는 제안한 기술이 3.2절에서 제시한 시스템 요구사항인 기밀성, 가용성, 데이터 정합성 및 무결성, 조건 검증 강제성에 대한 충족도를 평가한다.

5.1 기밀성

제안 기법의 기밀성은 속성 추천 단계와 암호화·재암호화 단계에서 확보된다. 문서 내용은 로컬 클라이언트 또는 내부 보호 영역에서 임베딩 벡터로 변환되며, 이 과정에서 사용되는 LLM 인코더는 내부 환경에서 실행된다. 임베딩 벡터는 속성 추천 과정에서만 활용되고 외부로 전송되지 않는다. 예를 들어 문서 내 사건 단계나 요청 권한 등이 벡터 공간에서 가장 근접한 속성으로 매칭되어 정책 구성에 필요한 후보 속성으로 선정된다.

선정된 속성은 암호화 단계에서 프록시 재암호화의 조건값으로 반영된다. 구체적으로 추천된 속성값에 해시 함수를 적용하여 조건 스칼라 값을 생성하고, 생성된 조건 스칼라 값은 세션 난수와 결합되어 사용자의 공개키의 지수부에 더해지는 형태로만 사용된다. 이 과정에서 저장소 운영자나 프록시는 암호문과 조건의 조합만 확인할 수 있으며, 조건의 상세 정보와 평문은 확인할 수 없다.

기존 환경에서의 문서 공유 및 접근제어는 문서와 접근정책이 분리된 채 관리되기 때문에 전달 과정에서 정책 누락이나 기준 불일치가 발생할 수 있다. 제안 기술에서는 문서를 기반으로 추천·선정된 속성이 암호화 단계에서 조건 값으로 직접 결합되므로 문서가 어떤 경로로 전송되더라도 조건을 충족하지 못하는 사용자는 복호화할 수 없다. 이를 통해 문서 전달 과정과 무관하게 정책의 일관성을 유지할 수 있다.

또한 서버 비밀값과 사용자 비밀 조각은 분리되어 관리되며, 단일 주체는 완전한 비밀키에 접근할 수 없도록 시스템이 설계되었다. 이를 통해 재암호화, 조건 변경, 복호화 전 과정에서 평문 복원은 적합한 속성과 키를 가진 요청자만 가능하며, 프록시와 저장소는 암호문과 제한적인 메타데이터만 활용한다. 이와 같은 구조를 통해 저장소 탈취, 프록시 로그 분석, 조건 변경 오용 등 공격 시나리오에 대해 문서 기밀성을 유지할 수 있다.

5.2 가용성

제안 기법은 실제 공조수사 환경에서의 긴급 문서 공유 상황을 고려하여, 장애 상황에서도 서비스가 지속 가능하도록 설계되었다. 이를 위해 프록시 계층은 단일 서버가 아닌 다수의 프록시 노드로 구성되며, 서버 공통 비밀값을 Shamir 비밀 분산 기법으로 분할하여 각 노드에 분산 저장한다. 일부 프록시 노드에 장애가 발생하더라도 임계값 이상의 노드가 유지되는 경우 재암호화 및 조건 변경이 가능하며, 이는 특정 노드 또는 저장소 장애로 시스템이 중단되는 상황을 방지할 수 있다.

조건 변경 과정에서는 콘텐츠 제공자가 문서의 접근 정책을 수정할 때, 기존 조건 스칼라 값과 새로운 조건 스칼라 값의 차이만 프록시에 전달함으로써 평문 복호화 없이 암호문 내부의 지수부를 갱신할 수 있다. 이에 따라 이미 저장된 암호문을 다시 암호화하거나 재업로드할 필요 없이, 단일 연산으로 조건 변경이 가능하므로 운영 효율성과 응답성이 향상된다.

www.kci.go.kr

속성 추천 과정에서도 임베딩 벡터와 정책 정보를 캐시화하여 대량 문서 처리 상황을 대비한다. 이를 통해 사용 빈도수가 높은 속성 및 문서에 대한 재연산을 최소화하고, 배치 처리 및 우선순위 기반 스케줄링을 통해 트래픽 집중 시에도 지연을 완화할 수 있다. 이러한 설계를 통해 제안 기법은 실무 환경에서 요구되는 서비스 연속성과 접근 가능성을 제공한다.

5.3 반신뢰

제안 기법에서 서버 공통 비밀값은 Shamir 비밀 분산을 통해 조각으로 분할되어 각 프록시 노드에 분산 저장된다. 이를 통해 임계값 미만의 프록시 노드가 공모하더라도 공통 비밀값을 복원할 수 없어 비밀 보호를 보장할 수 있다. 또한, 개별 사용자의 개인키는 서버 측에서 관리하는 값과 사용자 단말에서 생성되는 값의 합으로 정의되므로, 프록시 또는 사용자 단말만 탈취하는 것으로 완전한 개인키 확보는 불가능하다.

재암호화 단계에서 프록시는 재암호화에 필요한 부분 지수값이나 중간 파라미터만 계산하며, 최종 복호화에 사용되는 지수 값에는 단독으로 접근이 불가능하다. 조건 스칼라값과 세션 난수의 결합구조 역시 명시적으로 노출되지 않기 때문에, 프록시는 암호문을 다른 사용자용 암호문으로 변환하는 기능만 수행한다. 그 결과 프록시는 평문을 복원하거나 조건 구조를 재구성할 수 없어, 반신뢰 환경에서 요구되는 보안 수준을 달성할 수 있다.

5.4 데이터 정합성 및 무결성

제안 기법의 암호 설계 단계에서 암호문을 구성하는 값들은 조건 스칼라 값, 세션 난수, 서버 및 사용자 비밀 조각과 연관되어있다. 그러므로 공격자가 전송 또는 저장 과정에서 암호문 구성 값을 임의로 변조할 경우, 복호화 과정에서 요구되는 지수 관계가 충족되지 않아 평문 복호화는 불가능하다. 이를 통해 데이터 정합성과 무결성을 만족한다.

또한, 재암호화, 조건 변경, 복호화 요청에 대한 이력을 분산 원장에 저장하여, 동일 암호문에 대한 비정상적인 반복 요청, 암호문 구성 값 불일치 등의 이상행위를 탐지할 수 있다. 이를 통해 제안 기법은 암호 설계 단계에서의 구조적 무결성과 운영 단계에서의 로그 기반 이상 탐지를 결합함으로써, 데이터 정합성과 무결성을 기술적·관리적 측면에서 동시에 확보한다.

5.5 조건 검증 강제성

제안 기법은 속성 기반 조건 암호화 단계에서 조건 값을 별도의 평문으로 사용하지 않고, 지수부에 은닉된 형태로 표현한다. 즉, 문서 속성 벡터와 문맥 정보에 해시 함수를 적용해 도출한 조건 스칼라값은 세션 난수, 서버 비밀 조각, 사용자 비밀 조각과 결합되어 올바른 속성과 키를 가진 사용자만 상쇄할 수 있는 지수 형태로 표현된다. 콘텐츠 요청자는 자신의 비밀 조각과 프록시로부터 제공된 서버 관련 지수를 이용하여, 지수 값을 재구성하고, 그 역원을 암호문에 곱하여 복호화를 진행한다. 이 과정에서 콘텐츠 요청자의 속성이 암호화에 사용된 정보와 상이할 경우, 조건 스칼라 값이 틀려 지수부 상쇄가 실패한다. 콘텐츠 요청자는 이 과정에서 어떠한 조건이 불일치했는지에 대한 정보는 확인할 수 없어, 속성 조합 및 정책 추론이 불가능하다.

결과적으로 제안 기법은 속성 및 문맥 조건을 암호 시스템 내부 지수 연산에 통합함으로써, 조건 검증을 강제하는 동시에 조건 자체를 숨기는 특성을 동시에 달성한다. 이는 애플리케이션 계층에서의 단순 접근 차단 방식보다 강한 보안 보장을 제공하며, 문서 단위 및 업무 라인 단위의 세밀한 접근 제어를 실현하는 기반을 제공한다.

www.kci.go.kr

6. 결 론

본 논문에서는 명시적인 조직 정책표가 존재하지 않거나 충분하지 않은 환경에서 수사 문서 기반 접근 제어를 지원하기 위해, LLM 임베딩 기반 속성 추천 기법과 비밀 분산 기법을 결합한 조건은닉 프록시 재암호화 기법을 제안하였다. 먼저 한글 PDF 수사 문서를 중심으로 문서 - 속성 라벨 데이터셋을 구축하고, 문서 인코더와 속성 인코더로 구성된 임베딩 모델을 통해 문서와 속성을 동일 임베딩 공간에 투사함으로써, 실제 업무에서 관찰되는 경험적 정책을 반영하는 속성 후보 상위 K개를 자동 추천하는 방법을 제시하였다. 이를 통해 관리자가 직접 정책을 정의하지 않더라도, 문서 맥락과 조직 정보를 반영한 접근 속성 후보를 효율적으로 도출할 수 있다.

또한, 추천된 속성과 문맥 정보를 해시하여 생성한 조건 스칼라 값을 암호문 지수부에 은닉하고, 서버 비밀값을 Shamir 비밀 분산 기법을 이용하여 프록시 집합에 분산함으로써, 반신뢰 환경에서 조건은닉 프록시 재암호화를 수행할 수 있는 암호 프로토콜을 설계하였다. 제안 프로토콜은 단일 프록시 노드 또는 저장소가 탈취되더라도 평문이나 조건 값을 직접 복원할 수 없도록 하며, 속성 조건을 만족하는 사용자만이 복호에 성공하도록 함으로써, 암호화 단계에서부터 접근 정책을 강제하는 구조를 제공한다. 제안 기법은 조건 변경 시 평문 복호화 없이 암호문 내부의 조건 관련 지수부만 갱신할 수 있어, 변화하는 공조 수사 환경에 유연하게 대응할 수 있다는 장점이 있다.

제안 기법은 문서가 활용되는 전 구간에서 평문 노출을 최소화하여 기밀성을 유지하고, 다수 프록시 노드를 활용한 비밀 분산 기법을 통해 시스템의 가용성과 반신뢰 환경을 구축하였다. 또한, 암호문 구성요소와 비밀 조각, 조건 스칼라 등을 활용한 암호 설계와 분산 원장 기반 이력 관리를 통해 데이터 정합성과 무결성을 확보하고, 정확한 속성을 가진 사용자만 복호화가 가능한 암호화 프로세스를 통해 조건 검증 강제성을 제공한다.

향후에는 조건 스칼라 생성, 암호화, 재암호화, 복호화 단계 각각에서의 연산 소요시간을 측정하여 기존 PRE, C-PRE, AB-PRE 대비 오버헤드가 어느 수준인지 비교 평가할 예정이며, 저장소 탈취·프록시 로그 분석·조건 위변조 등 악성 시나리오를 구성하여 평문 노출 가능성이 존재하는지 검증 실험을 수행할 계획이다. 또한 수사 기관·콘텐츠 보호 기관과의 시범 적용을 통해 제안 기법의 실성능과 운영 편의성을 평가하고, LLM 기반 속성 추천 과정에서의 편향 및 설명 가능성을 고려한 정책 튜닝 기법을 연구할 계획이다. 마지막으로 텍스트 중심 문서에서 영상·음원 등 비정형 콘텐츠로 대상을 확장하여 국제 공조 수사 환경에 적용 가능한 통합 접근 제어 기술로 발전시키고자 한다.

본 연구는 문화체육관광부 및 한국콘텐츠진흥원의 2025년도 문화기술 연구개발 사업으로 수행되었음(과제명 : 한류콘텐츠 보호를 위한 국제공조수사 협력 체계 기술 개발, 과제번호 : RS-2024-00439553, 기여율 : 100%)

참 고 문 헌

[1] Danaher, Brett, and Michael D. Smith. “Gone in 60 seconds: The impact of the Megaupload shutdown on movie sales”, International Journal of Industrial Organization 33, 2014, DOI: 10.1016/j.ijindorg.2013.12.001

[2] Liu, Lei, Mingwei Cao, and Yeguo Sun. “A fusion data security protection scheme

www.kci.go.kr

for sensitive E-documents in the open network environment", Plos one 16.12, 2021, DOI: 10.1371/journal.pone.0258464

[3] United Nations Office on Drugs and Crime (UNODC), "Guidance on the Management of Criminal Justice Information", 2018.

[4] Atlam, Hany F., et al. "Risk-based access control model: A systematic literature review", Future Internet 12.6, 2020, DOI: 10.3390/fi12060103

[5] Zhao, Wayne Xin, et al. "A survey of large language models", arXiv preprint arXiv:2303.18223 1.2, 2023, DOI: 10.48550/arXiv.2303.18223

[6] M. A. K. Raiaan, Md. S. H. Mukta, K. Fatema, N. M. Fahad, S. Sakib, M. M. J. Mim, J. Ahmad, M. E. Ali, and S. Azam, "A Review on Large Language Models: Architectures, Applications, Taxonomies, Open Issues and Challenges", IEEE Access, vol. 12, 2024, DOI: 10.1109/ACCESS.2024.10433480

[7] Zhang, Jie, et al. "When llms meet cybersecurity: A systematic literature review", Cybersecurity 8.1, 2025, DOI: 10.1186/s42400-025-00361-w

[8] C. Song, L. Ma, J. Zheng, J. Liao, and H. Kuang, "Audit-LLM: Multi-agent collaboration for log-based insider threat detection", arXiv preprint, 2024, DOI: 10.48550/arXiv.2408.08902.

[9] H. Xu, S. Wang, N. Li, K. Wang, and Y. Zhao, "Large language models for cyber security: A systematic literature review", ACM Computing Surveys, 2024, DOI: 10.1145/3769676.

[10] A. Beimel, "Secret-sharing schemes: A survey", Coding and Cryptology, IWCC 2011 (LNCS 6639), Springer, pp.11 - 46, 2011, DOI: 10.1007/978-3-642-20901-7_2

[11] Y. Yang, S. Liu, C. Lee, Z. Gao, X. Yang, "Threshold Key Escrow Service with Intermediary Encryption", Proceedings of the 17th International Conference on Cryptology and Network Security (CANS 2023), pp.475-494, Springer, 2023, DOI: 10.1007/978-981-97-0798-0_27

[12] N. Andola, et al., "Proactive threshold-proxy re-encryption scheme for secure data sharing on cloud", Journal of Supercomputing, 79(13), pp.14117 - 14145, 2023, DOI: 10.1007/s11227-023-05221-3

[13] G. Ateniese, et al., "Improved proxy re-encryption schemes with applications to secure distributed storage", ACM Transactions on Information and System Security (TISSEC), 9(1), pp.1 - 30, 2006, DOI: 10.1145/1127345.1127346

[14] X. Liang, et al., "Attribute based proxy re-encryption with delegating capabilities", Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (ASIACCS'09), pp.276 - 286, 2009, DOI: 10.1145/1533057.1533094

[15] J. Lai, R. H. Deng, and Y. Li, "Expressive CP-ABE with partially hidden access structures", Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (AsiaCCS'12), pp.18 - 19, 2012, DOI: 10.1145/2414456.2414465

[16] Z. Hu, W. Susilo, J. Baek, J. Wu, "Conditional Proxy Pool Re-Encryption Scheme Against Chosen-Ciphertext Attacks", Proceedings of the 18th ACM Asia Conference on Computer and Communications Security (AsiaCCS 2023), pp.unknown, ACM, 2023, DOI: 10.1145/3596871.3596875

[17] Hynek Kydlíček, Guilherme Penedo, and Leandro von Werra. Finepdfs. https://huggingface.co/datasets/HuggingFaceFW/finepdfs, 2025. 3

www.kci.go.kr

저 자 소 개

박경엽(Kyung-Yeob Park)

2019.02 : 서울과학기술대학교 컴퓨터공학과 석사
2019.01-현재 : 엘에스웨어㈜ 소프트웨어연구소 연구개발본부 선임연구원
<주관심분야> 정보보호, IoT 보안, 블록체인, 빅데이터, 분산신원증명, 저작권 기술

김현수(Hyun-Soo Kim)

2019.02 : 단국대학교 소프트웨어학과 졸업
2023.08 : 숭실대학교 AI·SW융합학과 석사
2024.03-현재 : 숭실대학교 AI·SW융합학과 박사과정
2019.01-현재 : 엘에스웨어㈜ 소프트웨어연구소 연구개발본부 연구팀장
<주관심분야> 인공지능, 머신러닝, 컴퓨터 비전, 분산신원증명, 빅데이터

최창준(Chang-Jun Choi)

2019.02 : 상명대학교 컴퓨터공학과 졸업
2021.08 : 세종대학교 정보보호학과 석사
2021.09-현재 : 엘에스웨어㈜ 소프트웨어연구소 연구개발본부 선임연구원
<주관심분야> 정보보호, 블록체인, 네트워크 보안, 분산신원증명, 저작권 기술

신동명(Dong-Myung Shin)

2003.02 : 대전대학교 컴퓨터공학과 박사
2001-2006 : 한국정보보호진흥원 응용기술팀 선임연구원
2006-2014 : 한국저작권위원회 저작권기술팀 팀장
2014-2016 : 한국스마트그리드사업단 보안인증팀 팀장
2016-현재 : 엘에스웨어㈜ 소프트웨어연구소 연구개발본부 연구소장/전무이사
<주관심분야> 오픈소스 라이선스, 저작권 기술, 시스템/네트워크 보안, SW 취약점 분석·감정, 블록체인 기술

www.kci.go.kr