PASCON 2023
2023 공공 · 금융 · 기업 정보보안&개인정보보호 컨퍼런스

AI 기술을 활용한 개인정보 보호와 데이터 보안 시작하기

2023.09

FASOO

PASCON 2023
2023 공공 · 금융 · 기업 정보보안&개인정보보호 컨퍼런스

비식별화 준비하세요? 이건 꼭 알고 하셔야 합니다!

Contents

Ⅰ Check 1. AI 의 발전과 현재

Ⅱ Check 2. 규제와 국내외 동향

Ⅲ Check 3. AI 기술을 활용한 데이터 보호 방법

I

Check 1. AI 발전과 현재

1. AI 시대의 시작과 AI 서비스 활용
2. AI 필요성과 한계
3. 생각보다 가까운 AI활용
4. AI를 활용한 업무 활동

FASOO

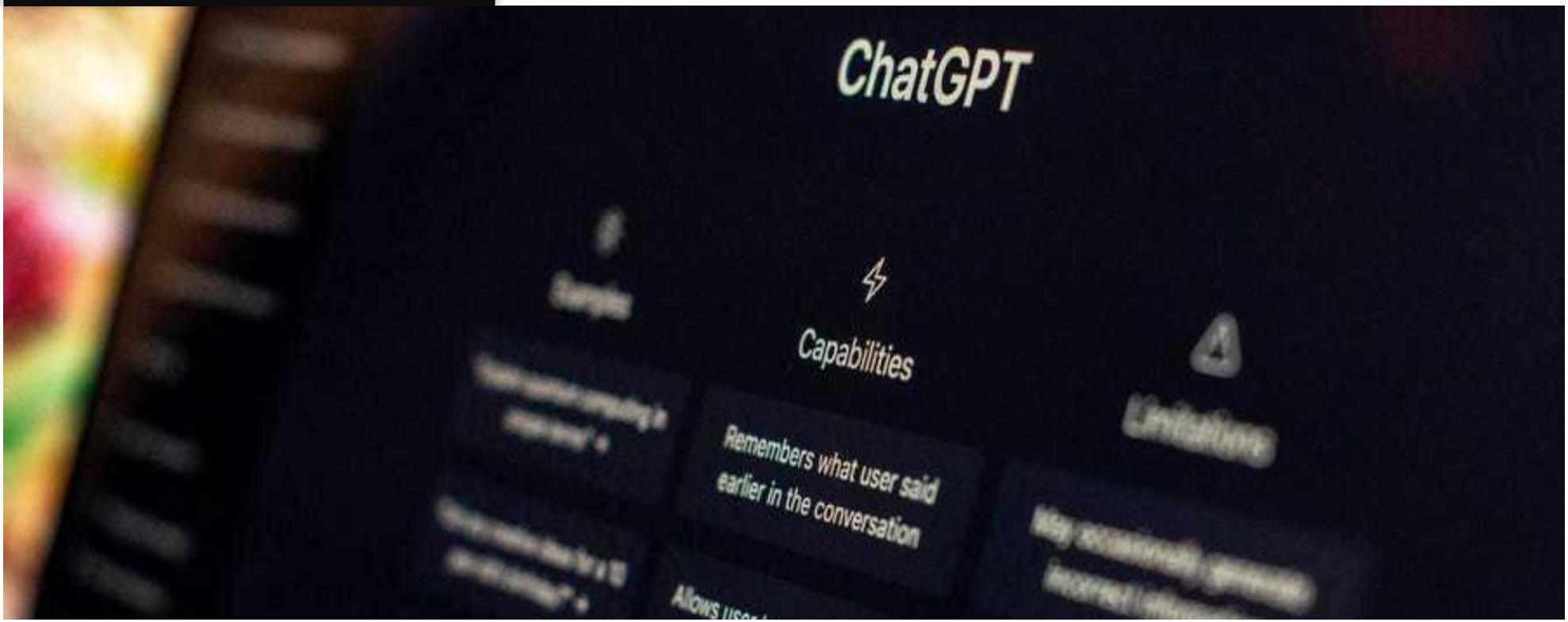
Check 1. AI의 발전과 현재

01 AI 시대의 시작과 AI 서비스 활용

AI는 4차 산업혁명 시대를 맞아 핵심으로 자리 잡았고 빠르게 진화하면서 우리 생활속에 빠르고 파괴력 있게 스며들고 있습니다.
산업 전반에서는 노동 비용의 절감과 새로운 일자리 창출, 노동자의 생산성 향상을 기대 하고 있습니다. 기업 및 기관에서는 도입에 대한 관심을 갖고 있으며 활용법에 대한 고민을 하고 있습니다.

생성형 AI의 시작

※ OpenAI가 개발한 프로토타입 대화형 인공지능 챗봇으로 ChatGPT는 대형 언어 모델 기반으로 만들어짐



Check 1. AI의 발전과 현재

02 AI 필요성과 한계

코로나 이후 디지털 전환이 가속화되고 데이터의 중요성이 점차 높아지고 있는 가운데, 산업 전반에 AI 기술을 적극 활용하는 사례가 늘어나고 있다. IBM이 발표한 '2022년 글로벌 AI 도입 지수(Global AI Adoption Index)'에 따르면 전체 기업의 35%가 AI를 활용하고 있으며 42%의 기업들도 도입을 적극 검토하고 있는 것으로 조사됐다.

AI 내재화의 어려움

AI 이니셔티브를 성공적으로 운영하는 것은 매우 어렵다

AI 역량 내재화 과정에서 고려하는 사항. ⓒ 코그넷나인

Check 1. AI의 발전과 현재

03 생각보다 가까운 AI 활용

"동네슈퍼까지 파고 든 AI…외주 끊고 생산성 UP" 챗GPT 효과로 인해 각 산업에 빠르게 적용되고 있습니다. 콘텐츠를 제작하거나 재고 관리를 하고 상품 추천까지 하고 있습니다. 또한 다소 어렵게 접근해야 했던 전문 영역까지 빠르게 침투하고 있습니다.
법률 분야 서비스를 하거나 해외 판례나 계약서를 번역하는 일까지 회사내 법무팀에서는 활용 중입니다.
AI를 적용하여 혁신적인 의사결정을 하는데 도움이 될 것 입니다.

AI를 활용한 기업 사례

AI는 생각보다 멀지 않고 어렵지 않게 활용이 가능하다.

기업	적용 기술	활용 분야
G마켓·아모레퍼시픽 등	브이캣	광고 영상·배너 자동 제작
KB라이프생명	디오비스튜디오	가상인간 광고 제작
위메이드플레이	자체 AI 애니	캐릭터 이미지 제작
브랜디·롯데온	업스테이지	상품 추천
김앤장 등 6대 로펌	베링랩	법률 번역
삼성생명·한화생명	업스테이지	보험금 자동 청구

그래픽 이진경

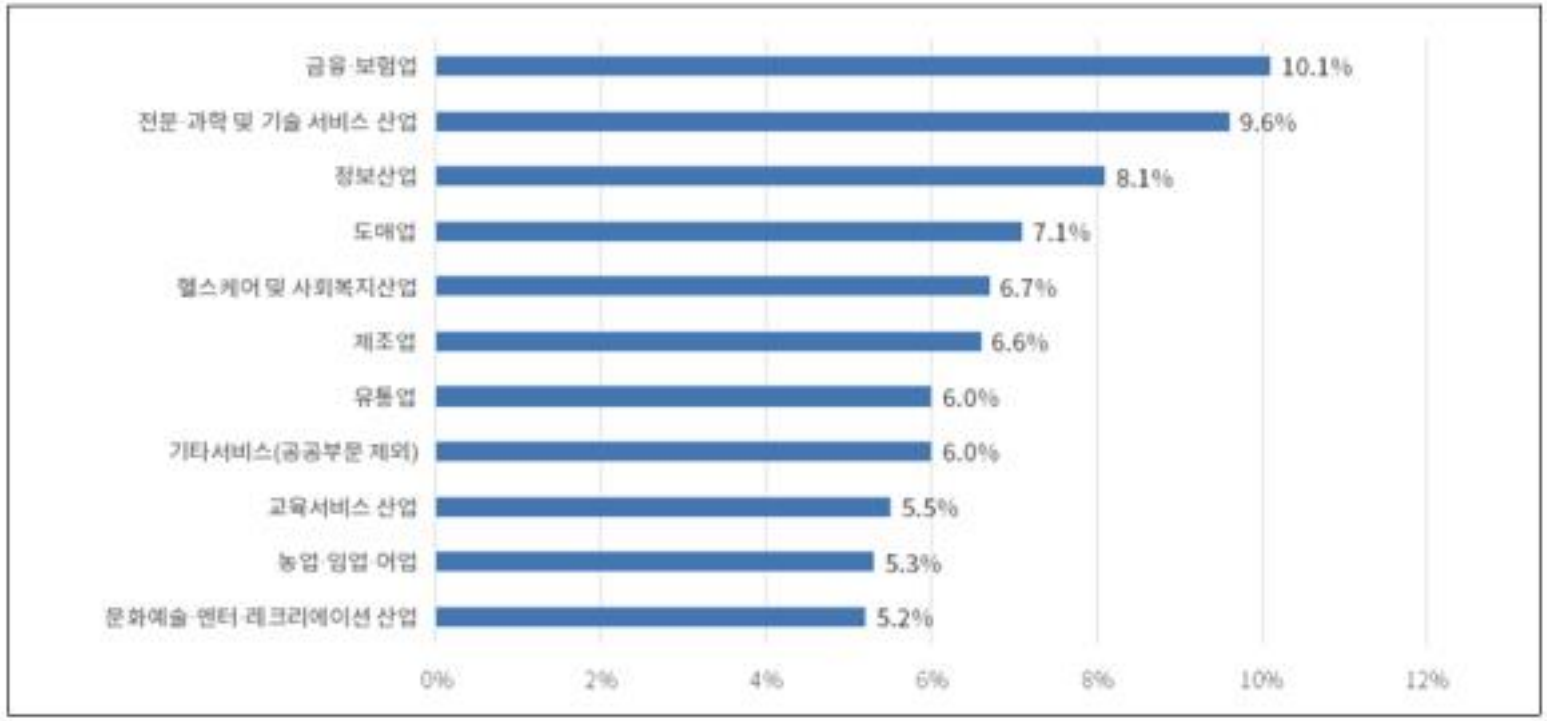
Check 1. AI의 발전과 현재

04 AI를 활용한 업무 활동

사람 보다 AI가 더 빠르게 처리할 수 있는 분야별로 업무활동에 적용되고 있습니다. 내부 업무에 활용하는 사례는 이미 증명되었고 효과를 체감하고 있습니다. 반복적인 업무를 하는 것과 또는 사람이 직접 하는 것보다 더 생산성이 있는 일에 적용하기 위한 새로운 좋은 방법입니다.

AI의 업무활동 영향 정도(%)

많은 기업들은 AI 기반의 업무 처리 로 효과를 받고 있습니다.



II

Check 2. 규제와 국내외 동향

1. 생성형 AI의 보안 위협
2. 국내/외 AI 정책 동향

FASOO

Check 2. 규제와 국내외 동향

01 생성형 AI의 보안 위협

"보안 전문가 85%, 생성형 AI로 인해 사이버 공격 늘었다" AI는 업무 생산성에 혁신을 제공 했지만 많은 불안 요소들을 갖고 있습니다. 이런 문제로 관심에서 활용 넘어가지 못하고 주저하는 현상이 발생 되었습니다.

대표 보안 위협	주요 원인	가능한 보안 위협
잘못된 정보	• 편향 • 최신 데이터 학습 부족 • 환각 현상	• 사회적 혼란 조장 • 고위험 의사 결정 • 잘못된 의사 결정 유도
AI 모델 악용	• 적대적 시스템 메시지	• 피싱 이메일 및 인물 도용 • 사이버 보안 위협 코드 작성 • 대화형 서비스를 악용한 사이버 범죄 • 커뮤니티 활성화 • 사회 공학적 영향 • 가짜 뉴스 생성
데이터 유출	• 데이터 합성 과정의 문제 • 과도한 훈련 데이터 암기 문제 • 대화 과정에서 개인정보 및 민감 • 정보 작성	• 훈련 데이터 유출 • 데이터 불법 처리 우려 • 기밀 유출 • 대화 기록 유출 • 데이터베이스 해킹 및 회원 추론 공격
유사 AI 모델 서비스 빙자	• 유사 악성 서비스 접근 유도	• 스쿼팅 URL 및 확장 프로그램 • 가짜 애플리케이션
확장 프로그램 취약점	• 확장 프로그램 내부의 악성 서비스 설치 • 서비스 제공 업체의 보안 조치 미흡	• 개인정보 수집 • 시스템 공격 • 호스팅 서버 및 스토리지 시스템 위협
API 취약점	• 미흡한 API 키 관리 • 데이터와 명령 사이의 불분명한 경계	• API 키 탈취 • 악의적인 프롬프트 주입

Check 2. 규제와 국내외 동향

02 국내/외 AI 정책 동향

해외 동향

(EU) 유럽 연합은 2023년 5월 11일 인공지능에 대한 세계 최초의 규제 프레임워크인 '인공지능 법(AI Act)'제정의 첫 단계로서 해당 법 초안을 유럽의회 상임위원회에서 통과시켰다.

- EU 인공지능 법에 따르면, 챗GPT 등 대규모 언어모델 및 생성 AI와 같은 이른바 '기초 모델(foundation models)' 제공업체 개발자는 모델을 공개하기 전에 안전 점검, 데이터 거버넌스 조치 및 위험 완화 조치를 적용해야 한다.
- 시스템을 훈련하는데 사용되는 학습 데이터 셋을 공개하고 생성 AI가 만든 콘텐츠는 인간이 생성한 것이 아님을 밝혀야 한다는 조항을 추가하였다.

(미국) 美 백악관 과학 기술 정책실(Office of Science and Technology Policy)은 2023년 8월 개최되는 데프콘(DEFCON)에서 챗GPT를 비롯한 생성형 인공지능 시스템을 공개 평가하여 잠재적인 취약점(potential harms)을 테스트한다고 밝혔다.

- 여기서는, 대규모 언어모델을 포함한 다양한 생성 AI에 내재한 혼란(confabulations), 탈옥, 편견과 같은 위험을 발견하고, 기업 개발자가 발견된 문제를 해결하도록 장려 하는 것을 목표로 한다.

(캐나다) 캐나다 개인정보 보호 규제당국(Canada privacy regulators)은 2023년 5월 26일 챗GPT의 모기업인 OpenAI의 데이터 수집 및 사용에 관한 공동 조사를 시작하였다.

– 연방 개인정보 보호 규제기관은 퀘벡, 브리티시 컬럼비아, 앨버타의 규제 기관과 함께

OpenAI가 챗GPT를 통해 사용자(residents)의 개인정보 수집, 사용 및 공개에 대한 동의를 얻었는지 여부를 조사할 것이라고 밝혔다.

국내 동향

「국가정보보안기본지침」 제15조 제1항 제19호에 의거, 첨단 정보통신기술을 활용한 정보화사업을 추진하기 위해서는 국가정보원의 사전 보안성 검토 절차를 준수하여야 한다.

내부망 구축시

- AI 모델을 적용·활용하기 위한 내부 업무 시스템은 인터넷 등 외부망과 분리된 상태로 운영되어야 한다.
- 기관 자체의 AI 모델을 학습·강화·가공 등 지속 개발·서비스할 수 있다. AI 모델 학습에 이용되는 기관 데이터 및 사용자 질의문·생성물등 개발·운용 시 발생하는 데이터는 기관 외부로 직접적으로 이동할 수 없다.

외부망 구축시

- 외부 공개 업무에 활용할 경우 AI 모델 학습에 필요한 기관 데이터 유출이 야기될 수 있으므로 충분한 주의가 필요하다.
- 정부 기관 소유 정보시스템상에서 상용 AI 모델을 도입하여 관련 서비스를 개발하고자 하는 경우, 학습에 이용되는 데이터 및 사용자 질의문 등 개발·운용 시 발생하는 모든 데이터에 대한 기관 자체 보안등급 분류를 통해 상용 AI 모델을 도입할 수 있는지 여부를 판단하여야 하며, 개발 이후에도 주기적 데이터 등급 지정·점검을 통해 철저한 관리가 필요하다

Ⅲ

Check 3. AI 기술을 활용한 데이터 보호 방법

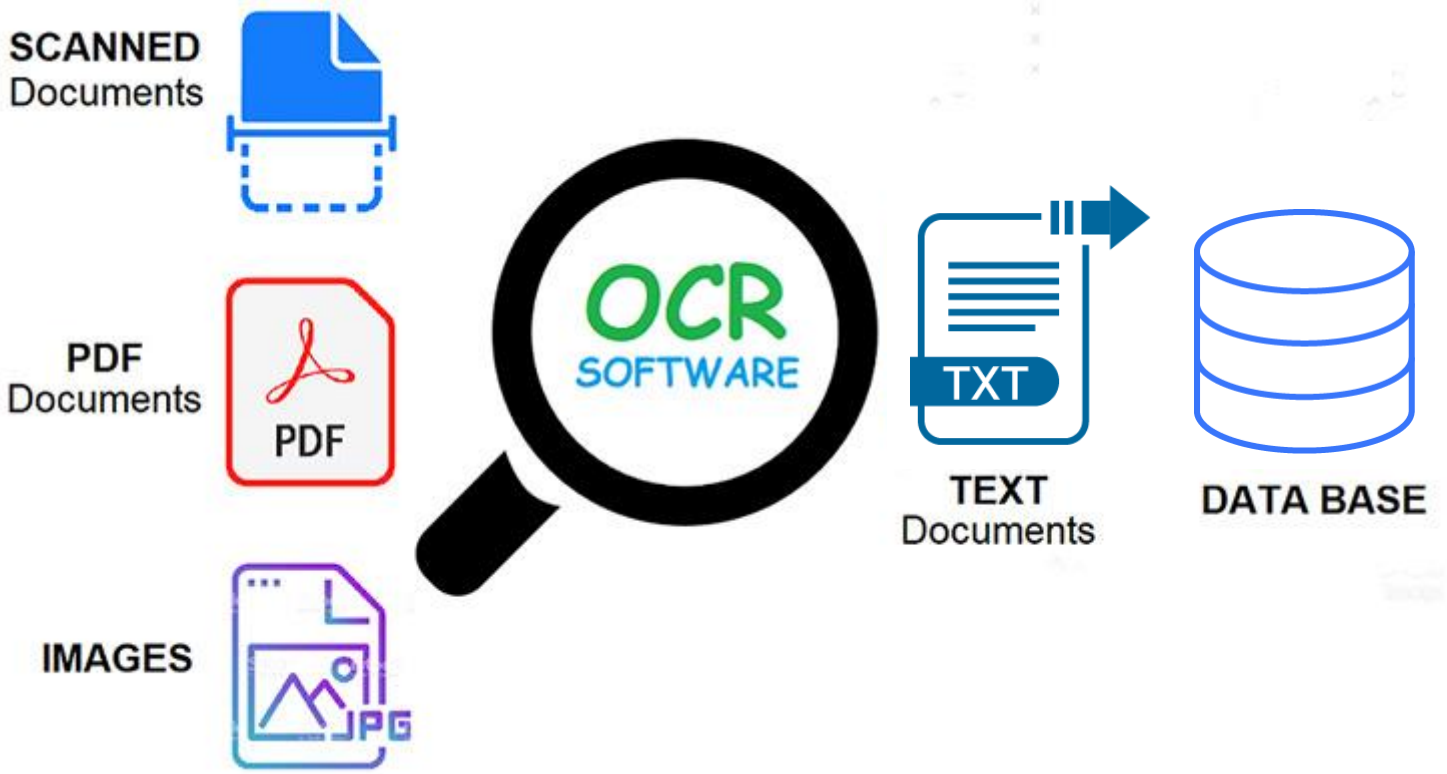
1. AI OCR
2. AI OCR
3. **Named Entity Recognition (NER)**
4. Data Masking
5. 안전하게 AI 서비스 사용하기
6. LLM으로 가는길? 출발은 데이터 관리부터

FASOO

01

Check 3. AI 기술을 활용한 데이터 보호 방법

AI OCR



Check 3. AI 기술을 활용한 데이터 보호 방법

02 AI OCR

Traditional OCR

Extract data from structured docs

Requires manual efforts for template settings

AI-powered OCR

Extract data from unstructured docs & images

Machine learning structures, extracts data, and insights from complex data

03

Check 3. AI 기술을 활용한 데이터 보호 방법

Named Entity Recognition (NER)

데얀 쿨루셉스키 인명/별명 (21 나이)가 해리 케인 인명/별명 (29 나이)에게 전한 말이 화제다. 20일 날짜 쿠팡플레이 IT 서비스 용어 가 공개한 토트넘 스포츠단체 방한 인터뷰 영상에서 쿨루셉스키 인명/별명 는 케인 인명/별명 에게 영상 편지를 띄워 " 손흥민 인명/별명 이 프리킥 스포츠 용어 을 차야 한다"고 주장했다. "안녕 해리 인명/별명 형, 나 쿨루셉스키 인명/별명 야"라고 입 동물 신체 부위 을 연 쿨루셉스키 인명/별명 는 "난 형이 전 세계 최고 스트라이커 중 하 인원수 나 개수/빈도 라고 생각해. 그런데 우리가 수요일 날짜 경기(팀 K리그전 스포츠 행사)에서 프리킥 스포츠 용어 을 차야 한다면 쏘니 인명/별명 가 차야 할 것 같아"라고 말했다. 옆 방향 에서 지켜보고 있던 손흥민 인명/별명 은 얼굴 동물 신체 부위 을 감싸 쥐며 소리 높여 웃었다. 함께 참석한 벤 데이비스 인명/별명 또한 웃었다. 이 영상은 SNS를 통해 현지 토트넘 스포츠단체 팬들 사이에서 큰 화제를 모으고 있다. 쿨루셉스키 인명/별명 가 웃으면서 하는 말이었지만 ' 뼈 세포/조직/기관 가 있는 말'이라는 반응이다. 지난 시즌 토트넘 스포츠단체 홋스퍼 스포츠단체 에서 프리킥 스포츠 용어 키커 스포츠 포지션 로는 케인 인명/별명 과 에릭 다이어 인명/별명 가 나섰다. 하지만 두 선수 인원수 는 한 골 개수/빈도 도 넣지 못했다. 토트넘 스포츠단체 이 이번 시즌 기록한 직접 프리킥 골 스포츠 용어 은 단 1개 개수/빈도 인데, 손흥민 인명/별명 이 넣은 골이다

04

Check 3. AI 기술을 활용한 데이터 보호 방법

Data Masking

구분	주민등록증	운전면허증
마스킹 항목	- 주민등록번호 뒷자리 6 자리 (940521-1******) - 발급일자 전체 : (****.**.**)	- 운전면허번호 뒷자리 6 자리 (12-34-56****-**) - 주민등록번호 뒷자리 6 자리 (940521-1******) - 일련번호 전체 : (******) - 발급일자 전체 : (****.**.**)

05

Check 3. AI 기술을 활용한 데이터 보호 방법

안전하게 AI 서비스 사용하기

AI 서비스는 기하급수적으로 늘어납니다. 규제와 보안의 문제로 시대의 흐름을 거스를 수 없습니다. 좋은 서비스를 안정적으로 운영하고 서비스 받기 위해서는 보안 수준을 끌어 올려야 합니다.
이용 가능한 서비스와 사용할 수 없는 서비스를 관리해야 하며 사용자별 접근 권한 정책을 부여해야 합니다.

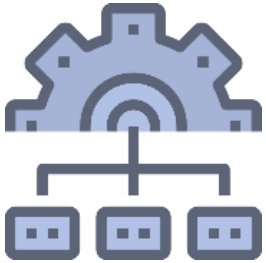
Fasoo AI-R DLP

06

Check 3. AI 기술을 활용한 데이터 보호 방법

LLM으로 가는길? 출발은 데이터 관리부터

국내 정보통신 기업들이 기업용 맞춤 거대언어모델(LLM) 인공지능(AI)을 연이어 개발하고 있습니다. 보안 문제를 해결할 수 있고 기업내 특화되게 활용 할 수 있는 AI가 필요하기 때문입니다. 기업 내부 정보를 정보보호 문제 없이 분석할 수 있습니다.
좋은 모델이 될 수 있도록 충족하기 위해서는 특화된 맞춤 데이터가 필요합니다. 또한 접근할 수 없는 데이터의 보호도 필요합니다.



최신 버전의 문서를
정확히 파악하여 학습에 활용

필요없는 중복 문서를
제거하여 품질높은 데이터 활용

컨텐츠 내용과
문서의 메타 정보를 활용


PASCON 2023
2023 공공 · 금융 · 기업 정보보안&개인정보보호 컨퍼런스
감사합니다.
FASOO