FIELD AI (2)



금융회사 Usecase 맞춤형 비식별화 및 위험평가리포트 생성 인공지능

목차

01 아이디어 소개

- 아이디어개요
- 아이디어 제안 배경

02 모델링

- 데이터 및 모델 활용
- 아이디어 실현

03 서비스 강점

- 아이디어의 독창성
- 문제해결 가능성
- 발전 가능성

1-1. 아이디어 개요

(1) 금융회사 cs : 금융 도메인 특화 인 비정형 데이터 (2) 비정형 데이터 (2) 비정형 데이터 (3) 반당 수준, 방법 추천 : 연구목표를 저해하지 않는 선에서 가명 처리 수준 결정 (4) 부천 및 자동화 검플라이언스 (4) 비식별화, 가명처리 평가 보고서 (5) 가명처리 요구사항 충족 및 보고서 출력

FIELD AI Pipeline



Why

1. 가명처리

- : 데이터 활용 시 가명처리 의무 존재
- 2. 금융 비정형 데이터 : 다량의 금융 데이터가 축적되었으나 실질적 활용이 어려운 상황 (2021년 300만 건)

What

1. FIELD의 가치

: 보안 + 자동화 + 전문성

- 2. FIELD의 기능
- 1) 데이터 항목 분류, 비식별화
- ▶ 비식별화 대상 항목 구분, 가명정보 형태로 비식별화
- 2) 데이터 항목 식별위험성 평가
- ▶ RAG 공식 검증된 정보 참조, 가명처리 판단 근거
- 3) 가명처리 수준/방법 추천
- ▶ RAG 기반 적절한 가명처리 방법 추천

How

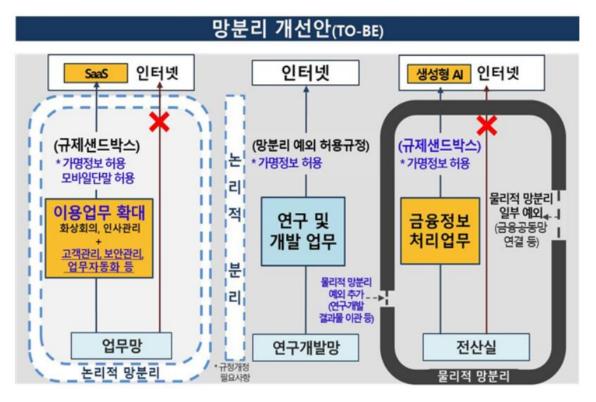
Input: Raw data (ex. 통화내역)

- 1) 데이터 항목 분류, 비식별화
- **▶** NER
- ▶ 로컬 LLM 1차 처리 후 외부 API 연계
- 2) 데이터 항목 식별위험성 평가
- ▶ 공식 가이드라인 기반 RAG
- ► Groundedness Check
- 3) 가명처리 수준/방법 추천
- ► 다른 SI/보안기업 비식별화 솔루션과의 연계

Output: 위험평가보고서(.xlsx)

#1. CS 비정형 데이터 활용 시 가명 처리 필요 (데이터 3법 개정)

금융보안원 [[금융분야 망분리 개선 로드맵]] (2024.8) 해외 소재 생성 AI 사용 가능 but 가명 정보만 허용



Problem : 비정형 데이터의 가명처리 어려움

Solution 1. Private LLM

Solution 2. Other LLM API (ex.GPT)

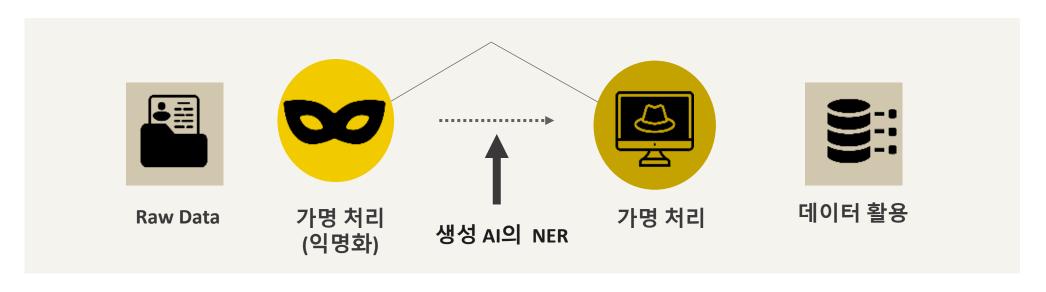
Hybrid de-identification

출처: 금융보안원 홈페이지

#2. 효과적인 가명처리 방법론

Stepwise pseudonymization

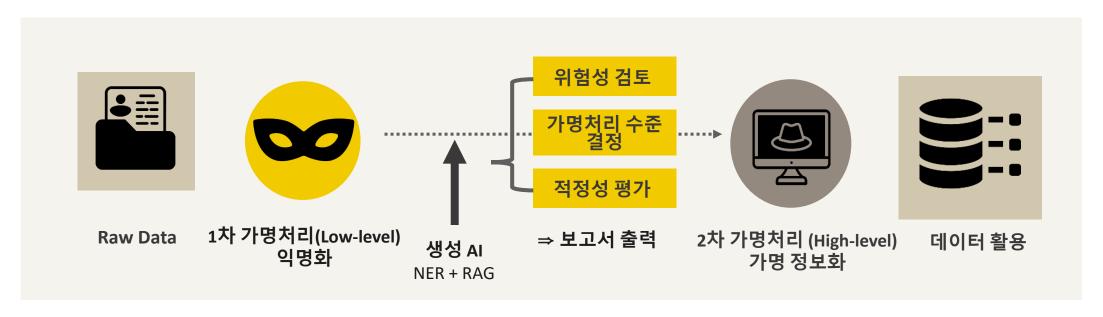
1차 가명처리 vs 2차 가명처리 차이점 : 익명화 vs 가명화로 비식별화 수준과 방법론 차이



#3. Value-Add

Compliance-ready

요구되는 컴플라이언스를 한 번에 해결



2-1. 데이터 및 모델 활용

Data





KLUE



De-identification Model



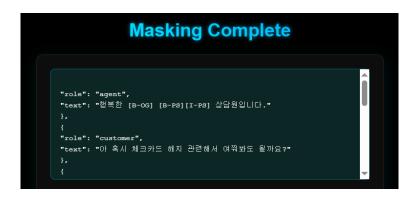
Risk Report Model







Masked Data



Risk Report

항목명	구분	설명
성함 1	식별자	상담원의 이름 정보를 식별합니다.
성함 2	식별자	고객과 상담원이 성함을 주고받는 대화 중에서 식별된 고객 명칭으로, 고객 응대 시 일관성과 개인화된 서비스를 제공하기 위해 필요한 정보입니다.
은행 이름	개인식별가능정보	대화에서 언급된 고객의 은행 이름입니다.
계좌번호	식별자	고객의 체크카드와 연결된 은행 계좌번호를 식별합니다.
카드번호	식별자	고객이 소유한 체크카드의 식별 번호입니다. 이는 여러 금융 서비스와 계좌 정보와 연결될 수 있으며, 고객의 금융 활동을 관리하는 데 필수적입니다.
전화번호	식별자	고객이나 상담 업무에서 확인을 위해 사용되는 연락쳐 정보입니다. 상담 시 은행 문의 및 서비스 해지 절차 안내에 이용됩니다.
카드사 이름	개인식별가능정보	고객의 데이터 항목 중 카드사 이름에 대한 정보를 의미합니다.
기타 항목	개인식별가능정보	성담원이 고객 문의에 대해 해당 카드와 계좌 정보를 안내하는 대회입니다. 성담 과정에서의 고객 계좌 잔액 확인 방법 및 절차, 이 대화에서는 고객이 체크카드 해지 전에 카드와 연결된 계좌의 잔액을 확인하려 하지만, 직접 잔액 조회는 불가능하고 은행에 직접 문의해야 한다는 안내를 받습니다. 상담원은 계좌가 외화계 좌인자 여부 확인 역시 고객이 은행 클센터로 문의해야 한다고 설명합니다.

Raw Data
행복한 가나다은행 홍길동 상담원입니다.
임꺽정 고객님 본인 맞습니까?
1234 5678 9012
가나다은행 123 4567891234 계좌



Masked Data					
행복한 [BANK] [NAME] 상담원입니다.					
[NAME] 고객님 본인 맞습니까?					
[CARD]					
[BANK] [ACCOUNT] 계좌					

항목명	개인 식별 위험	위험성 평가 근거 체크리스트 번호 및 상세 내용	가명처리 필요 여부	비식 별화 방법 (번호)	비식별화 방법명	적용 방법 및 논리 설명
상담원 이름	중간	(①) 그 자체로 특정 개인을 식별 할 가능성이 있음	필요	1	휴리스틱 익명화	'부록 1. 가명·익명처리 기법'과 '식별자 삭제 또는 대체' 방법을 참조하여, 상담원 이름을 일 반 명칭
고객 이름	높음	(①) 그 자체로 특정 개인을 식별 할 가능성이 있음	필요	1	휴리스틱 익명화	고객 이름을 가명 예: 고객A, 고객B로 대체하여 분석 시 고객 특정 방지.
체크카드 번호	높음	(①) 그 자체로 특정 개인을 식별 할 가능성이 매우 높음	필요	3	암호화	금융 분야의 가명익명처리 안내서에 따르면, (2021-12-28, p.22-24) 암호화는 데이터의 재 식별 가능성을 최소화하면서도 가명정보 보호
계좌번호	높음	(①) 그 자체로 특정 개인을 식별 할 가능성이 매우 높음	필요	3	암호화	금융분야에서는 계좌번호를 매우 민감한 개인식별 정보로 취급. "금융분야 가명익명처 리 안내서"(2021, p.36)에 의거하여 암호화를 추천함.

De-identification





INPUT

Raw Data 행복한 가나다은행 홍길동 상담원입니다. 임꺽정 고객님 본인 맞습니까? 1234 5678 9012 가나다은행 123 4567891234 계좌

데이터항목 분류

항목명 	
상담원 이름	
고객 이름	
카드번호	
계좌번호	

1차 익명화

Masked Data
행복한 가나다은행 [NAME] 상담원입니다.
[NAME] 고객님 본인 맞습니까?
[CARD NUMBER]
가나다은행 [ACCOUNT] 계좌

Risk Report





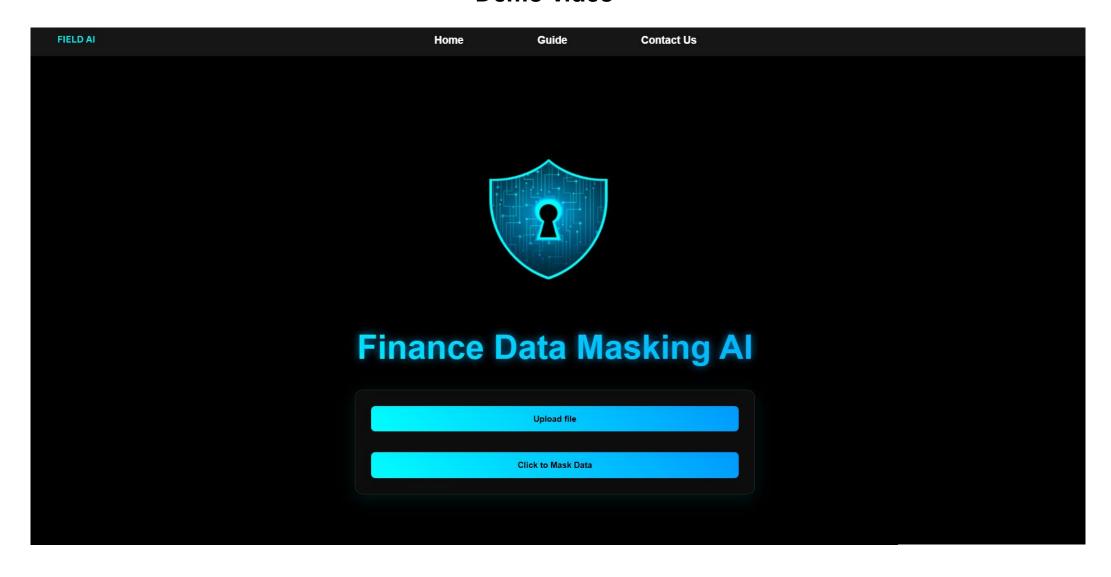
1차 익명화

Masked Data 행복한 가나다은행 [NAME] 상담원입니다. [NAME] 고객님 본인 맞습니까? [CARD NUMBER] 가나다은행 [ACCOUNT] 계좌

위험평가리포트 생성

항목명	개인 식별 위험	위험성 평가 근거 체크리 스트 번호 및 상세 내용	가명서 리 필요 여 부	별화	비식별화 방법명	적용 방법 및 논리 설명
상담원 이 름	중간	(①) 그 자체로 특정 개인 을 식별할 가능성이 있음	필요	1	휴리스틱 익명화	'부록 1. 가명·익명처리 기법'과 '식별자 삭제 또는 대체' 방법을 참조하여, 상담원 이름을 일반 명칭
고객 이름	높음	(①) 그 자체로 특정 개인 을 식별할 가능성이 있음	필요	1	휴리스틱 익명화	고객 이름을 가명 예: 고객A, 고객B로 대 체하여 분석 시 고객 특정 방지.
체크카드 번호	높음	(①) 그 자체로 특정 개인 을 식별할 가능성이 매우 높음	필요	3	암호화	금융 분야의 가명익명처리 안내서에 따르면, (2021-12-28, p.22-24) 암호화는데이터의 재식별 가능성을 최소화하면서도 가명정보 보호
계좌번호	높음	(①) 그 자체로 특정 개인 을 식별할 가능성이 매우 높음		3	암호화	금융분야에서는 계좌번호를 매우 민감한 개인식별 정보로 취급. "금융분야 가명 익명처리 안내서"(2021, p.36)에 의거하 여 암호화를 추천함.

Demo video



3-1. 아이디어 독창성

Service differentiation

금융도메인 Fine tuning

- 다양한 금융 관련 데이터셋 학습
- 금융보안원보고서기반RAG생성

올인원 Solution

- 데이터 비식별화 및 보고서 생성 동시 진행
- 단일 Pipeline 구성

안전한외부AI

- AI에 개인정보 마스킹된 데이터 전달
- 개인정보유출가능성 원천차단

비정형 데이터 통합

- 활용이 제한되었던 비정형 데이터 특화서비스
- 텍스트,음성데이터모두적용가능

3-2. 문제해결가능성

Current Problem & Solution

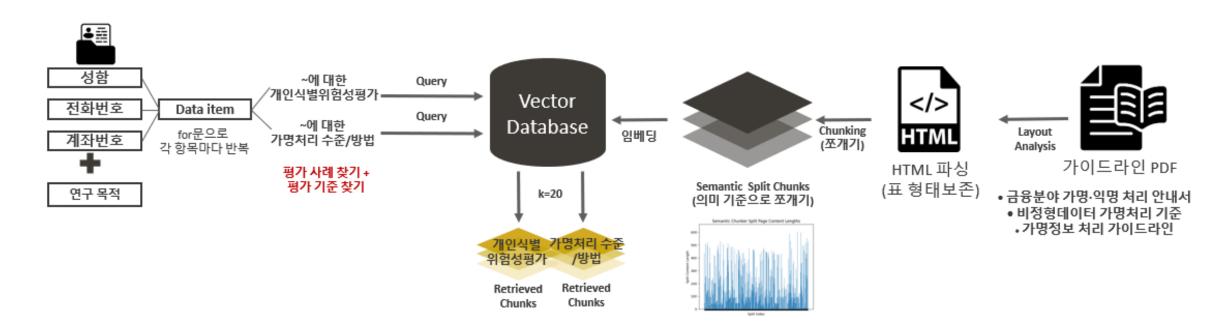
항목 Problem		Solution
현행 가명처리 문제	비정형데이터 활용의 어려움	개인정보 마스킹을 통한 비정형 데이터 활용 용이
현행 가명처리 문제	항목별 위험성과 가명처리 수작업	NER 모델, 생성 AI 자동화
생성 AI 보안 문제	생성 AI 사용시 개인정보 유출 문제	로컬 LLM / 외부 API 구분, 2단계 마스킹
보고서 생성 Risk	Hallucination	RAG, Groundness Check

3-2. 문제해결가능성

Quality Control

데이터 항목별로 위험성 평가, 가명처리 수준 및 방법 결정 반복

1) RAG

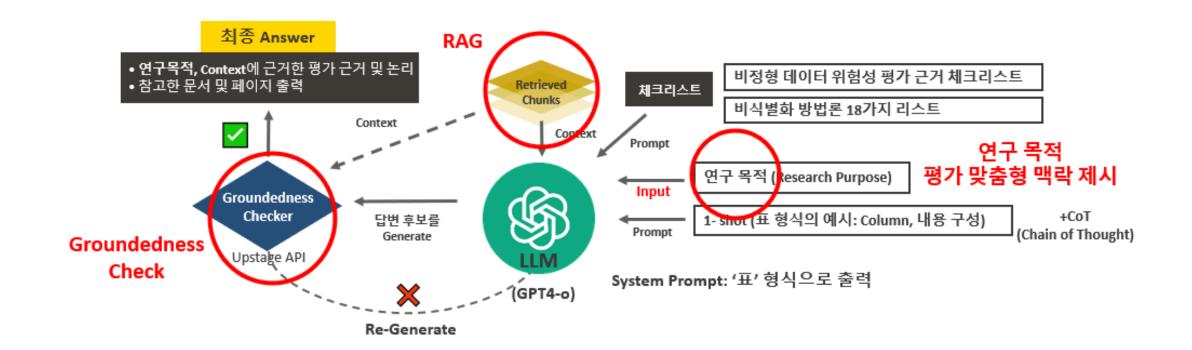


3-2. 문제해결가능성

Quality Control

데이터 항목별로 위험성 평가, 가명처리 수준 및 방법 결정 반복

2) Groundedness Check

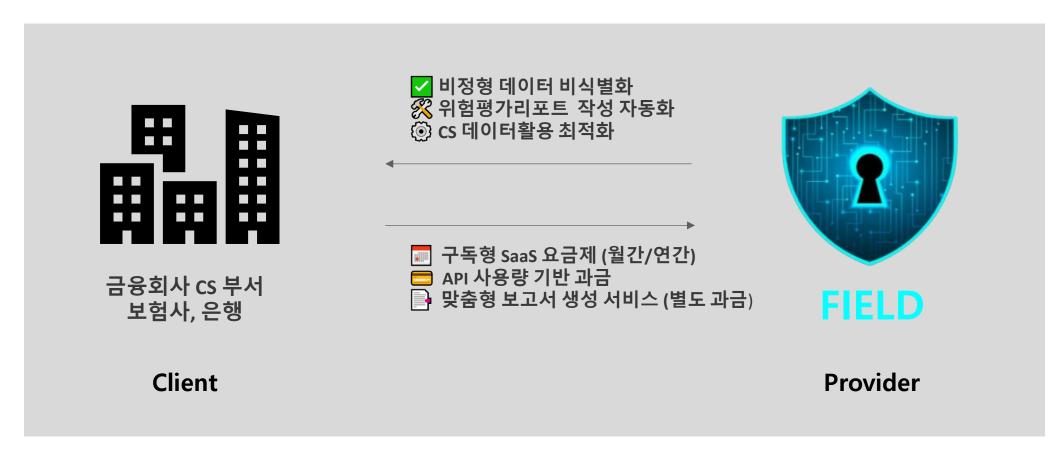


3-3. 발전 가능성

Further Development

B2B SaaS 솔루션 최신 법령 동기화 보안 강화 규제 업데이트 모니터링 API 연동 지원 강화 사용자 접근 제어 강화 보고서 생성 맞춤 옵션 제공 리스크 예측 모델 적용 이중 인증(2FA) 도입 모듈화된 사용자 인터페이스 법령 검색 기능 추가 데이터 추적성 강화

Business model(B2B)



FIELD AI

Thank you.