2025 금융 AI Challenge : 금융 AI 모델 경쟁

개요

[배경]

금융 분야의 AI 활용 활성화를 지원하고 전문인력을 양성하기 위해 **'2025 금융 AI Challenge : <Track1> 금융보안 특화 AI 모델 경쟁'**를 개최합니다.

이번 대회를 통해 금융보안에 특화된 데이터 분석 및 활용 역량을 강화하여 전문 인력을 양성하고, 금융권의 AI 활용 어려움에 따른 해결 방안을 함께 모색하며 금융 산업의 AI 활용 활성화를 지원하는 것을 목표로 하고 있습니다.

[대회 방식]

본 대회는 예선, 본선 그리고 최종 순으로 진행됩니다.

🔷예선 : 본선 진출팀을 선발하기 위한 과정이며 Private 리더보드 상위 12팀이 본선에 진출하게 됩니다.

🔷본선 : 본선 진출팀은 코드와 결과 보고서를 제출하고 내부 평가를 진행합니다. 본선 평가 상위 6팀이 최종에 진출하게 됩니다.

🔷최종 : 최종 진출팀은 발표 자료를 제출하고 발표 평가를 진행합니다. 최종 평가 상위 4팀이 최종 수상자로 선정됩니다.

※ 최종 평가는 오프라인 발표 평가로 진행됩니다.

[주제]

금융보안 실무에 적합한 개발 방법론 및 AI 모델을 발굴하기 위해 FSKU 평가지표를 기반으로 AI 모델의 성능을 경쟁

[설명]

FSKU 평가지표 문항 세트(객관식 및 주관식)에 대해 정확한 응답을 생성하는 AI 모델을 개발

🔷Input: 선다형 질문 또는 주관식 질문

🔷Output: 정답 번호 또는 정확한 답변(Text)

※ 반드시 단일 LLM 모델에서 객관식과 주관식에 대한 응답이 모두 생성되어야 합니다.

[주최 / 주관 / 운영]

주최/주관: 금융보안원

후원: 금융위원회

공동개최사: 하나은행, 신한은행, 카카오뱅크, 미래에셋증권, 신한카드

운영: 데이콘

[참가 대상]

AI에 관심 있는 누구나

(개인 또는 4인 이내 팀 구성 가능)

평가

1. 예선 리더보드

- **평가 산식**
- **객관식 점수** : 정확도
- 정확도(Accuracy): (정답 일치한 객관식 개수) / (전체 객관식 개수)

$$\text{Accuracy} = \frac{\text{정답과 일치한 객관식 문항 수}}{\text{전체 객관식 문항 수}}$$

- **주관식 점수** : 0.6 X 의미 유사도 + 0.4 X 키워드 재현율 기반 혼합 점수
- 의미 유사도(Cosine Similarity): 예측 문장과 정답 문장 간의 OpenAI 임베딩(text-embedding-3-small) 기반 코사인 유사도

$$\text{CosineSimilarity} = \cos(\theta) = \frac{\vec{E}_{\text{gt}} \cdot \vec{E}_{\text{pred}}}{\|\vec{E}_{\text{gt}}\| \cdot \|\vec{E}_{\text{pred}}\|}$$

- 키워드 재현율(Keyword Recall): 정답 키워드 중 예측 문장에 등장한 키워드 비율

$$\text{KeywordRecall} = \frac{|\{\text{예측 답변에 포함된 정답 키워드}\}|}{|\{\text{전체 정답 키워드}\}|}$$

- **Score = 0.5 x 객관식 점수 + 0.5 x 주관식 점수**

※ 의미 유사도 평가는 OpenAI 임베딩 API를 기반으로 수행됩니다. 해당 API는 floating-point 허용 오차 수준에서 변동이 있을 수 있습니다. 이로 인해 동일한 제출에서도 점수에 ±0.00005 내외의 미세한 변동이 발생할 수 있습니다.

- Public score : 전체 테스트 데이터(FSKU) 중 사전 샘플링된 50%
- Private score : 전체 테스트 데이터(FSKU) 100%

2. 평가

- **예선 평가** : 리더보드 Private Score **상위 12팀 선발**
- **본선 평가** : 예선 평가 선발 12팀 코드 및 결과보고서 제출 후 코드 검증 및 본선 내부 평가
- **추가 비공개 평가 데이터셋**에 대한 예측 결과 평가 80% + 결과보고서 서면 평가 점수 20%를 합산한 총점을 기준으로 **상위 6팀 선발**

평가	평가 항목	평가 방식	선발
2차 평가	객관식 점수 (50%)	리더보드 평가 산식	상위 6팀
	주관식 점수 (30%)	리더보드 평가 산식(50%) + 심사위원 정성 평가 (50%)	
	결과 보고서 점수 (20%)	설계 및 학습 과정에 대한 서면 평가	

🔷추가 비공개 평가 데이터셋: 리더보드 평가 데이터셋이 아닌, 참가자에게 공개되지 않은 별도의 추가 데이터셋

🔷예선 평가를 통과한 12팀은 코드를 제출하고, 심사위원이 이를 활용해 추가 비공개 데이터셋에 대해 직접 추론 및 평가를 진행합니다.

🔷주관식 문항에 대한 심사위원 정성 평가는 '생성된 응답의 표현력, 논리성, 문장 완성도, 실무 활용성' 등을 전문가로 구성된 심사위원단이 종합적으로 평가합니다.

심사 분야	심사 항목	평가 기준	배점
내용	타당성	- 기술 구현을 위한 접근 방식이 기술적·논리적으로 타당한가?	25%
	정확성	- 모델 구현에 대한 설명이 정확하게 이루어졌는가?	15%
	충실성	- 내용이 충실하게 작성되었고 결과가 명확한가?	10%
기술 (전문성)	데이터 적절성	- 금융보안 도메인에 부합하는 신뢰성 있는 데이터를 활용하였는가? - 검색 가능성과 문맥 유지 측면에서 벡터화·쪼개기(chunking)가 잘 처리되었는가?	20%
	설계	- 사용한 AI 모델이 주어진 문제에 적합한지, 모델의 선택이 타당한지, 모델의 설계가 잘 되었는지를 고려	15%
	구조	- 모델 학습 및 성능 개선 구성이 타당하게 설계되었는지, 모델 개선, RAG 등의 과정이 충분히 진행되었는지 평가	15%
합계			100%

🔷결과 보고서 점수는 위의 평가 항목에 의해 평가되며 총점의 20%가 2차 평가 총점에 반영됩니다.

- **최종 평가** : 본선 평가 선발 6팀 대상 후 **최종 상위 4팀 수상**

  오프라인 발표 평가

평가	평가 항목	평가 방식	선발
최종 평가	본선 점수 (70%)	본선 객관식 + 주관식 평가 총점	최종 4팀 수상
	발표 점수 (30%)	발표 자료 품질·활용 가능성 평가	

🔷발표는 발표자료(PDF)' 파일로 진행 (* 기술적 오류 방지를 위해 PPT는 허용되지 않음)

규칙

1. 참여

- 개인 또는 팀을 이루어 참여할 수 있습니다.
- 개인 참가 방법 : 팀 신청 없이, 자유롭게 제출탭에서 제출 가능
- 팀 참가 방법 : 팀 탭에서 가능, 상세 내용은 팀 탭에서 팀 병합 정책 확인
- 팀 구성 방법: 팀 페이지에서 팀 구성 안내 확인
- 팀 최대 인원: **4명**
- 동일인이 개인 또는 복수팀에 중복하여 등록 불가

2. 대회 규칙

1) LLM 기반 텍스트 생성 요건

- 최종 답변은 생성형 언어 모델(LLM)에 의해 생성된 텍스트여야 하며, 단순한 룰 기반 출력이나 사전 정의된 정답 목록에서의 선택만으로 구성된 응답은 허용되지 않습니다.
- 검색 증강 생성(RAG) 방식은 허용되나, 검색된 내용을 그대로 반환하는 방식은 불가하며, 생성 모델을 활용한 조합, 요약, 재구성 등의 가공이 반드시 포함되어야 합니다.

2) 사전 학습 모델 사용 가능 범위

- 2025년 8월 1일 전(~2025.07.31)에 공식적으로 가중치가 공개되었으며, 최소한 비상업적 이용이 허용된 오픈소스 라이선스(MIT, Apache 2.0 등)로 배포된 사전 학습 모델만 사용할 수 있습니다. 해당 조건을 충족하지 않는 모델은 사용이 불가능합니다.

3) API 사용 제한

- OpenAI API, Gemini API 등과 같이 원격 서버를 통해 응답을 받는 형태의 API 기반 모델은 사용할 수 없습니다. 모든 모델은 로컬 환경(CPU 또는 GPU 기반)에서 직접 실행 가능한 형태로만 사용해야 하며, 외부 서버(클라우드 등)에 의존하는 방식은 허용되지 않습니다.

4) 외부 데이터 사용 가능

- 2025년 8월 1일 전(~2025.07.31)에 공식적으로 공개되었으며, 최소한 비상업적 이용이 허용된 라이선스(CC BY-NC, CC0, CC-BY-SA, CC-BY-NC-SA 등)로 배포된 외부 데이터만 사용할 수 있습니다. 해당 조건을 충족하지 않는 외부 데이터는 사용이 불가능합니다.
- 직접 수집한 데이터(예: 수기 작성, 자체 크롤링)는 사용할 수 없습니다. 외부 데이터는 반드시 공식적으로 공개되어 있으며, 라이선스가 명확하게 부여된 경우에만 사용 가능합니다.
- 데이터 증강은 허용되며, 코드 상 구현이 가능한 방식으로 사용해야 합니다. 단, 증강에 활용된 원천 데이터와 사용된 모델 역시 대회 규칙2), 3)을 충족해야 합니다.

※ 데이터 증강 예시: Rule-Based 기반 Text 증강, 로컬에서 구동되는 생성AI 모델을 활용한 데이터 생성 등

🔷모든 외부 데이터는 출처, 사용 방식, 데이터 파일 등 증빙이 가능해야 하며, 이에 대한 확인이 이루어지지 않거나 라이센스가 저작권 침해 등 법적 문제가 있는 경우 실격 처리됩니다.

🔷모든 데이터 증강 과정은 관련 코드와 함께 제출되어야합니다.

5) 추론 코드는 제시된 리소스 내에서 제한 시간 내 작동할 수 있어야함

- 리더보드 결과를 재현할 수 있는 추론 코드는 아래 리소스 조건 내에서 작동할 수 있어야 합니다.

🔷제한 시간 : 전체 평가 데이터셋(FSKU)에 대하여 **4시간 30분(270분)**을 초과할 수 없습니다. (샘플 당 약 30초 내 추론)

추론 시간은 운영진이 직접 추론 코드를 5번 실행하여 소요된 시간의 평균으로 측정합니다.

🔷추론 환경(리소스) [Runpod 링크]

GPU: RTX 4090 24GB VRAM

CPU: 6 vCPU 41GB RAM

DISK: 40GB

주요 환경: Python 3.10, CUDA 11.8, Pytorch 2.1.0, Ubuntu 22.04

🔷추론 코드 내에는 모델 입력을 위한 데이터 전처리, 모델 로드, 모델 추론, 최종 출력 생성의 모든 과정이 포함되어 있어야 합니다.

🔷추론 코드는 인터넷 연결이 차단된 오프라인 환경 서버에서 진행되며, 추론 과정에서 인터넷 통신 과정이 포함될 수 없습니다.

6) 추론 모델은 반드시 단일 LLM 모델이어야함

- 추론은 반드시 단일 LLM 모델로 수행해야 하며, 복수의 LLM을 앙상블하거나 입력 유형(4지선다, 5지선다, 주관식)에 따라 다른 LLM을 사용하는 것은 허용되지 않습니다.

3. 코드 및 결과 보고서 제출 규칙

- 예선 종료 후 본선 평가 대상자는 아래의 양식에 맞추어 코드와 모델 체크포인트, 코드 실행 방법이 담긴 자료를 dacon@dacon.io 메일로 기한 내에 제출
- 제출한 코드는 대회 규칙을 준수하고 Private Score 복원이 가능해야 코드 검증 과정을 통과할 수 있습니다.

[제출 코드 관련]

🔷코드에 데이터 입/출력 경로를 상대 경로로 표기

🔷코드와 주석 인코딩: UTF-8

🔷모든 코드는 대회 규칙에서 제시된 리소스 환경에서 오류 없이 설치되고 실행될 수 있어야 함

🔷라이브러리 버전 기재 (requirement.txt)

🔷모델에 활용한 모든 외부 데이터와 전처리 코드를 필수로 포함 (외부 데이터 출처 증빙 포함)

🔷추론(Inference) 코드는 반드시 별도의 코드 파일로 작성(예시: inference.py 혹은 inference.ipynb)해야 하며, 추론에 활용하는 모델 가중치(Weight) 파일을 필수로 포함

[제출 파일 목록]

🔷Private Score 복원이 가능한 코드 (추론 코드는 반드시 별도로 구성)

🔷Private Score 복원이 가능한 모델 가중치(Weight) 파일

🔷사용한 외부 데이터 관련 증빙 자료

🔷결과 보고서

4. 유의 사항

- 1일 최대 제출 횟수: 3회
- 사용 가능 언어: Python
- 모든 csv 형식의 데이터와 제출 파일은 UTF-8 인코딩을 적용합니다.
- 모델 학습과 추론에서 평가 데이터셋 정보 활용(Data Leakage)시 수상 제외
- 대회 기간 내 팀 외의 모든 인사이트 및 코드 공유는 데이콘 플랫폼 내에서 공개적으로만 이루어져야하며 이 밖의 모든 비공식적인 공유 행위는 Private Sharing으로 간주합니다.
- 모든 학습, 추론의 과정 그리고 추론의 결과물들은 정상적인 코드를 바탕으로 이루어져야하며, 비정상적인 방법으로 얻은 제출물들은 적발 시 규칙 위반에 해당됩니다.
- 최종 순위는 선택된 파일 중에서 채점되므로 참가자는 제출 창에서 자신이 최종적으로 채점 받고 싶은 파일 1개를 선택해야 함
- 대회 직후 공개되는 Private 랭킹은 최종 순위가 아니며 코드 검증 후 수상자가 결정됨
- 데이콘은 부정 제출 행위를 엄격히 금지하고 있으며, 데이콘 대회 부정 제출 이력이 있는 경우 평가가 제한됩니다.
- 자세한 사항은 링크를 참고해 주시기 바랍니다.

5. 문의

- 데이콘은 대회 운영 및 데이터 이상에 관련된 질문 외에는 답변을 드리지 않고 있습니다. 기타 질문은 토론 페이지를 통해 자유롭게 토론해 주시기 바랍니다.
- 데이콘 답변을 희망하는 경우 [토크] 페이지 대회 문의 게시글에 댓글을 올려 주시기 바랍니다.

일정

[예선 일정]

- 참가 신청 기간 : 2025년 07월 14일(월) 14:00 ~ 2025년 08월 29일(금) 14:00
- 예선 기간 : 2025년 08월 01일(금) 14:00 ~ 2025년 8월 29일(금) 14:00
- 팀 병합 마감 : 2025년 08월 22일(금) 23:59
- 예선 종료 : 2025년 08월 29일(금) 14:00
- 본선 진출팀 발표 : 2025년 09월 01일(월) 14:00

[본선 내부 평가 일정]

- 코드 및 결과보고서 제출 마감 : 2025년 09월 12일(금) 23:59
- 코드 검증 및 본선 평가 : 2025년 09월 15일(월) 10:00 ~ 2025년 9월 26일(금) 10:00
- 최종 평가 대상자 안내 : 2025년 9월 29일(월) 14:00

[최종 발표 평가 일정]

- 발표 자료 제출 마감 : 2025년 10월 16일(목) 23:59
- 오프라인 발표 평가 : 2025년 10월 23일(목) 예정
- 최종 수상자 발표 : 2025년 10월 31일(금) 예정
- 오프라인 시상식 : 2025년 11월 20일(목) 예정

※ 세부 일정은 대회 운영 상황에 따라 변동될 수 있습니다

상금

[총 상금 3,300만 원]

<table>
<tr><th>수상 구분</th><th colspan="2">(트랙 I) 모델 경쟁</th><th colspan="3">(트랙II) 공모전</th></tr>
<tr><td>대상</td><td colspan="5">금융위원회 위원장상
(1,500만원)
※ 모델 경쟁 1등과 공모전 1등 중 한 팀 선정</td></tr>
<tr><td>최우수상</td><td colspan="5">금융보안원 원장상
(800만원)
※ 모델 경쟁 1등과 공모전 1등 중 대상에 선정되지 않은 한 팀</td></tr>
<tr><td>우수상</td><td>하나은행장상
(200만원)</td><td>신한은행장상
(200만원)</td><td>카카오뱅크
대표이사상
(200만원)</td><td>미래에셋증권
대표이사상
(200만원)</td><td>신한카드
대표이사상
(200만원)</td></tr>
</table>

🔷해당 대회 페이지는 <Track1> 모델 경쟁 대회입니다.

🔷수상자에게는 금융보안원 채용 특전 혜택이 제공됩니다.

🔷대상 및 최우수상의 경우, 2025 금융 AI Challenge의 <Track2> 공모전과 통합하여 1팀이 선정됩니다.

🔷관련 자세한 내용은 금융보안원 홈페이지(www.fsec.or.kr)에서 참고하실 수 있습니다.

※ 위 상금은 제세공과금이 포함된 금액으로 실지급액은 제외 후 지급될 예정입니다.

※ 세부 상금은 대회 운영상황에 따라 변동될 수 있습니다.

데이터

Dataset Info.

- **test.csv [파일]**
  - ID : 샘플별 고유 ID
  - Question

ID	Question
TEST_000	금융산업의 이해와 관련하여 금융투자업의 구분에 해당하지 않는 것은? 1 소비자금융업 2 투자자문업 3 투자매매업

	4 투자중개업 5 보험중개업
TEST_001	위험 관리 계획 수립 시 고려해야 할 요소로 적절하지 않은 것은? 1 수행인력 2 위험 수용 3 위험 대응 전략 선정 4 대상 5 기간
TEST_002	관리체계 수립 및 운영'의 '정책 수립' 단계에서 가장 중요한 요소는 무엇인가? 1 정보보호 및 개인정보보호 정책의 제·개정 2 경영진의 참여 3 최고책임자의 지정 4 자원 할당 5 내부 감사 절차의 수립
TEST_003	재해 복구 계획 수립 시 고려해야 할 요소로 옳지 않은 것은? 1 복구 절차 수립 2 비상연락체계 구축 3 개인정보 파기 절차 4 복구 목표시간 정의
TEST_004	트로이 목마(Trojan) 기반 원격제어 악성코드(RAT)의 특징과 주요 탐지 지표를 설명하세요.
TEST_005	한국은행이 금융통화위원회의 요청에 따라 금융회사 및 전자금융업자에게 자료제출을 요구할 수 있는 경우는? 1 전자금융거래의 보안 강화를 위해 2 전자금융거래의 통계조사를 위해 3 금융회사의 경영 실적 분석을 위해 4 통화신용정책의 수행 및 지급결제제도의 원활한 운영을 위해
TEST_006	개인정보보호법 제22조의2에 따라 만 14세 미만 아동의 개인정보를 처리하기 위해 필요한 절차로 옳은 것은? 1 아동의 학교의 동의를 받아야 한다. 2 법정대리인의 동의를 받아야 한다. 3 아동 본인의 동의만 받으면 된다. 4 아동의 친구의 동의를 받아야 한다.
TEST_007	전자금융거래법에 따라 이용자가 금융 분쟁조정을 신청할 수 있는 기관을 기술하세요.

TEST_008	금융권에서 SBOM을 활용하는 이유로 가장 적절한 것은? 1 금융 시스템의 접근 제어 정책을 효율적으로 구현하기 위해 2 금융 거래의 투명성을 높이기 위해 3 고객의 개인정보 보호를 강화하기 위해 4 금융 상품의 다양성을 확보하기 위해 5 S/W 공급망 공격을 예방하기 위해
TEST_009	전자금융거래법 제44조에 따르면, 청문 절차가 필요한 경우는 무엇인가? 1 전자금융거래의 중단 2 전자금융거래의 보안 점검 3 전자금융업자의 등록 취소 4 전자금융거래의 수수료 변경

- **sample_submission.csv [파일]**
  - ID : 샘플별 고유 ID
  - Answer : 예측한 답변