2024-2 상업정보교과논리논술

금융에서의 생성형 인공지능 활용 현황과 법적 쟁점에 대한 연구

컴퓨터교육과 2021312602 김민서
컴퓨터교육과 2021312602 노주희
컴퓨터교육과 2021310788 전혜진
컴퓨터교육과 2020310100 정소연

4조 : 금융도끼 은도끼 🪓

I. 서론

금융 분야에서 생성형 AI의 성장성

- 2022년 **약 8억 달러** → 2032년 **약 94억 달러** 성장 예상

  (연평균 28.1% 성장률).

- **사기 탐지, 보안 강화, 투자 예측** 등 다양한 금융 영역에서 활용 가능.

생산성 향상

- 생성형 AI를 활용하는 근로자의 생산성이 평균 14% 향상될 수 있음.
- 챗봇을 통한 고객 응대, 투자 보고서 작성 등의 **생산성 향상**과 **비용 절감** 기대.

I. 서론

법적 규율 부재

현재 **우리나라의 생성형 AI 관련 법적 규율이 전무**한 상황.

금융에서의 사용 현황과 예상되는 **법적 쟁점 검토의 필요성**이 강조됨.

Ⅱ. 생성형 AI의 의의와 현황

" 학습된 데이터를 기반으로
새로운 콘텐츠를 생성할 수 있는 딥러닝 모델 "

II. 생성형 AI의 의의와 현황

예측형 AI vs 생성형 AI

G2.com

Predictive AI

Data analytics method to train input dataset and use it to predict fresh data.

Generative AI

Generative adversial networks to identify patterns in old data to classify content.

전혜진

예측형 AI vs 생성형 AI

예측형 AI: **패턴을 분석**해 미래를 예측

생성형 AI: **새로운 콘텐츠를 생성**함.

BUT 예측형 AI와 생성형 AI는 상호보완적 관계로,

데이터 분석 및 콘텐츠 생성 능력을 함께 향상시킬 수 있음.

전혜진

금융 분야에서의 사용 현황

고객 서비스

- **챗봇** 등으로 고객의 요구에 신속하게 대응하며, 맞춤형 투자 추천 가능.
- **임베디드 금융**(비금융 플랫폼에서의 금융 서비스)에서 고객의 행동 데이터를 분석해 **맞춤형 서비스** 제공.

고객 투자 관리

- 포트폴리오 생성과 투자 전략 제안에 AI가 활용됨.
- 비대면 서비스를 통한 투자 전략 논의와 맞춤형 투자 추천이 가능해짐.

전혜진

금융 분야에서의 사용 현황

위험 관리

- **사기, 자금 세탁** 등의 이상 거래 포착에 AI가 활용됨.
- 대출 심사에서 신용 평가 및 위험 평가를 **자동화**하거나 **반자동화**하는 데 유용.

업무 개선

- 재무보고서 작성, 시장 분석, 금융상품 개발 등 **업무의 효율성**을 크게 향상.
- **금융 상품 개발** 및 **코드 작성** 지원으로 금융기관의 업무를 혁신.

생성형 AI 등에 대한 법적 규율 현황

우리나라의 법적 규율 부재

- 생성형 AI를 직접 규율하는 법은 없지만, **"인공지능 산업 육성 및 신뢰 기반 조성법"**과 **"인공지능 책임법"** 등이 국회에 계류 중.
- 개인정보 보호법 개정안 및 콘텐츠산업 진흥법 개정안 등이 일부 금융 영역에 적용될 가능성.
- 금융위원회의 **"금융분야 AI 운영 가이드라인"**(2021)은 AI 시스템의 **위험 관리**, **윤리 원칙 준수**, **공정성** 등을 강조.

전혜진

생성형 AI 등에 대한 법적 규율 현황

유럽연합(EU)

- "인공지능법(AI Act)"이 통과되어 AI를 **4단계로 위험성에 따라 규율**.
- 고위험 AI는 **신용도 평가, 생체 인식** 등 금융 관련 위험성 규제를 받음.

미국

- AI 관련 지원 법안이 있지만, **규제적 의미는 크지 않음**.

III. 생성형 AI의 개별적인 기술구조와 금융에서의 각각의 활용

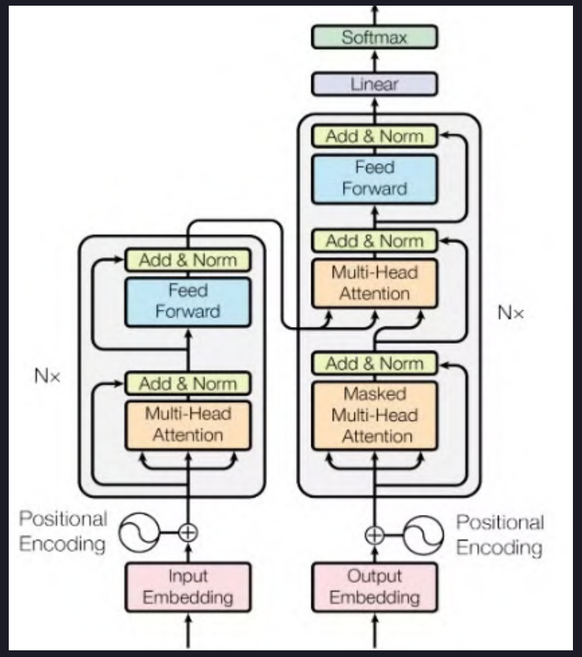
- 생성형 AI는 배포 초기 단계로 아직 기술적으로 미성숙한 상태
- But, 금융 공학과 AI의 기술이 빠르게 발전하고 있기 때문에 그 기술적 활용이 어떻게 진행될 지 섣불리 예측하기 힘듦.

→ 현재까지 나온 생성형 AI 모델들의 현황을 기반으로 구현이 가능한 금융 분야 3가지 소개

III. 생성형 AI의 개별적인 기술구조와 금융에서의 각각의 활용

1. GAN

대립하는 관계인 2가지
AI 모델, 생성기와 판별기를
동시에 사용하는 **비지도학습** 방법



2. Transformer

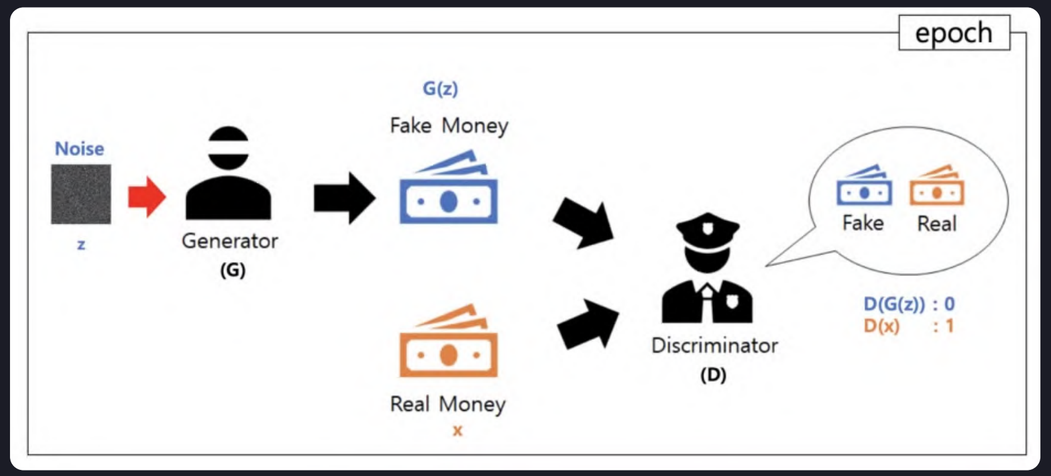
자기 주의 메커니즘(Self-attention)을 이용한 대규모 언어 모델(LLM)의 핵심 구조

3. 다중 모드 AI

이미지, 음성, 문자 등 다양한 데이터를 결합하여 더 정확한 분석을 제공하는 AI

1. 생성적 적대 신경망 (Generative Adversarial Networks : GAN)

생성기와 **판별기** 두 신경망이 서로 대립하여 훈련되는 구조의 신경망



금융에서의 활용 →

- **사기 거래 탐지**: 정상적인 거래 패턴과 비정상적인 패턴을 구분하여 사기를 탐지
- **악성코드 탐지**: 금융 보안에서 악성코드를 탐지하고 차단
- **데이터 편향 문제 해결**: 합성 데이터를 생성해 데이터 편향 문제를 완화

김민서

2. 트랜스포머 모델 (Transformer model)

대규모 언어 모델(LLM)과 생성형 AI의 기반을 마련한 것으로,
'자기 주의 기법'(Self-attention)을 활용

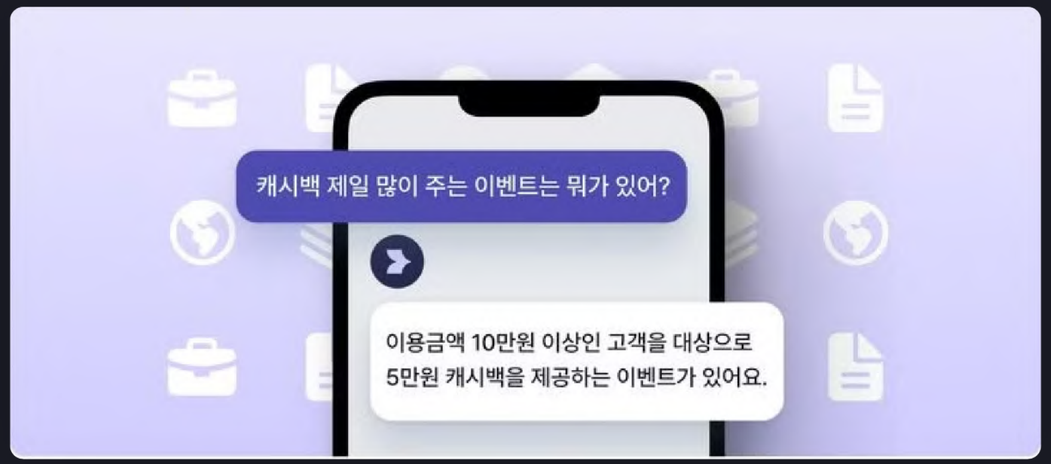
자기 주의 기법 (Self-Attention):
쿼리(Query), 키(Key), 밸류(Value) 세 가지 벡터를 통해 단어들 간의
관련성, 유사성을 측정하고, 각 단어의 중요도에 가중치를 부여해 상호작용을 강화하는 방식

금융에서의 활용 →

- **감정 분석:** 뉴스와 소셜미디어에서 시장 동향을 분석
- **금융 예측**: 시계열 데이터를 분석하여 주가, 금융 상품의 수요를 예측
- **재무 분석**: 재무 보고서 작성 자동화

3. 다중모드 AI (Multimodal) AI

이미지, 음성, 문자 등 여러 유형의 데이터를 결합해 통찰력 있는 결정을 내리는 AI 모델



금융에서의 활용 →

- **정확한 투자 판단**: 투자자 감정과 금융 지표를 결합하여 더 나은 투자 판단
- **신용 분석**: 회사 및 개인 신용도 평가에 감정 데이터를 포함한 종합적 분석
- **금융 업무 간소화**: 문서 작성, 광고 제작 등 자동화

IV. 금융법상 쟁점과 과제

1. 조작위험 (딥페이크)
2. 금융안정성의 위험
3. 투자자보호 관련 위험
4. 데이터 유출 위험
5. 불공정의 위험
6. 기타 쟁점

1. 조작위험(딥페이크)

딥러닝 + 페이크 (Fake)

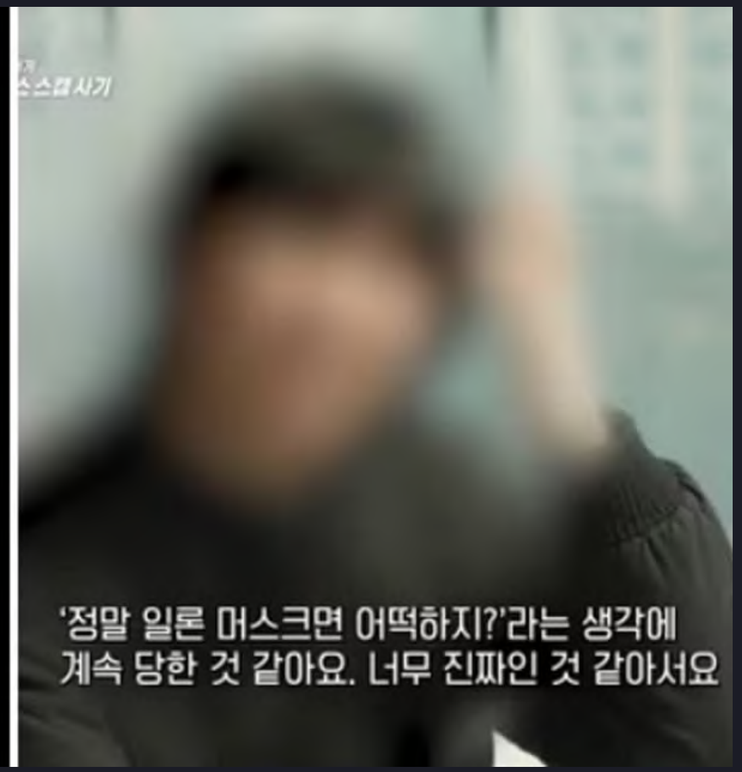
1. 금융 신원 도용으로 인한 **사기 피해**
2. 허위 거래정보 유포를 통한 **불공정거래**
3. 딥페이크를 이용한 **보이스피싱이나 메시지 피싱**

이외에도 악성코드 생성, 비밀번호 해독 등에 사용될 가능성

IV. 금융법상 쟁점과 과제

1. 조작위험(딥페이크)

딥러닝 + 페이크 (Fake)



조선일보
https://www.chosun.com › national_general › 2024/04/22

"난 일론 머스크, 사랑해"… 가짜 영상통화에 7000만원 뜯겼다

2024. 4. 22. — … **일론 머스크** 테슬라 최고경영자를 사칭한 소셜미디어 계정에 속아 7000만원을 뜯긴 한국인 피해자의 사연이 전해졌다 … **사기** 피해를 입었다. A씨는 작년 7 …

IV. 금융법상 쟁점과 과제

1. 조작위험(딥페이크) 대응방안

(1) 딥페이크 탐지

조작되었다는 점을 뒷받침할 만한 증거를 찾고 그 증거를 제시하는 기법

한계: 성능이 학습데이터셋에 의존, 오탐지(false-positive) 문제

ex. GPTZero, FakeCatcher

(2) 원본인증

원본에 고유정보를 입력하고 원본이 수정된 경우 고유정보도 변경되는 기법

한계: 인증 표준이 마련되지 않음

ex. 디지털 워터마크, 핑거프린팅, 해시정보 삽입

2. 금융 안정성의 위험

(1) 플래시 크래시

매도 물량이 대량으로 쏟아지는 경우

증시가 폭락하는 것

- 생성형 AI를 기초로 거래시스템을 구축하는 경우 플래시 크래시가 유발될 우려

ex. 2018년 2월 뉴욕증시폭락 사건

(2) 조작된 정보를 생성하는 AI

AI가 이익만을 달성하도록 설계한 경우

허수주문을 하거나 가장매매를 하는 등

시장을 조작할 우려

2. 금융 안정성의 위험 대응방안

현재 <자본시장법>이나 <가상자산이용자보호법>에는 AI가 자율적으로 시장을 조작하더라도 이를 규제할 방안이 없음

↓

1. 학습데이터나 알고리즘에 ***공정성 기준***을 부과
2. 사용자가 사전적 또는 사후적 관리 감독을 미이행할 경우 ***민사상 사용자책임***과 같은 과실 책임을 입법화
3. AI 개발자에게 <**제조물책임법**>과 같은 ***무과실책임***을 부과

3. 투자자 보호 관련 위험

(1) 투자권유 단계

AI를 활용하여 투자결정을 내리는 경우 이를 고객에게 이해시키지 않는다면 ***설명의무 위반*** 발생 우려

(2) 자산운용

기존에는 인간의 투자판단에 대해 ***선관주의의무***를 부과할 수 있었음

다만, AI가 직접 투자판단을 하는 경우 AI 의사결정 과정을 이해할 수 없다면 ***선관주의의의무***에 해당하는지 검토 어려움

3. 투자자 보호 관련 위험 대응방안

금융투자업자

- AI 훈련데이터셋,
  데이터 및 알고리즘 적정성 검토
- 외부침입이 없도록 보안 감사

외부기관

- 만약 금융투자업자에게 ***선관주의의무***
  위반 책임이 인정되기 어렵다면
  외부기관에 직접 <***제조물책임법***>상
  책임을 물을 수 있음
- 이를 방지하기 위해 외부기관은
  금융투자업자에게 AI의 특징, 한계 등을
  설명해야 함

4. 데이터 유출 위험

(1) AI 훈련용 데이터셋 외부 유출

- 이름, 주소 등 개인의 식별 정보나 신용카드 정보와 같은 민감한 정보를 노출

(2) 가명 or 익명화된 데이터 재식별되어 외부 유출

- 본래 가명 or 익명화된 데이터는 개인정보 추론이 어렵지만 여러 데이터셋 결합, 데이터마이닝 등을 통해 특정 개인을 재식별할 수 있음

(3) 프롬프트 노출에 따른 개인정보 유출

- 프롬프트에 질문하는 과정에서 고객정보가 들어갈 수 있고 이에 따른 외부 유출 위험

4. 데이터 유출 위험 대응방안

"합성데이터"

원본데이터를 사용하여 인위적으로 생성한 학습 데이터

[한계]

- 합성데이터가 기존의 데이터셋을 제대로 대표하지 못하면 오류 발생
- 회원추론 공격: 합성데이터를 역추론하여 원데이터를 드러내는 방식

IV. 금융법상 쟁점과 과제

5. 불공정의 위험

(1) 데이터 및 알고리즘 편향 (Bias)

성별, 인종, 연령에 따라 불공정하고 차별적인 결과를 산출할 수 있음

(2) 의사결정 이유의 설명 문제

AI가 내부적으로 어떻게 동작하는 지 인간은 이해 어려움
→ AI가 대출승인을 거부해도 그 이유를 고객에게 설명하기 어려움

(3) 자동화된 의사결정의 문제

고객은 자신의 데이터에 대해 사용동의를 하지 않았거나 그 수집방법을 예상하지 못했을 수 있음

5. 불공정의 위험 대응방안

(1) 데이터 및 알고리즘 편향 (Bias)

1. **투명성 조치**: 데이터 수집 및 처리과정을 공개
2. 윤리적 데이터 수집
3. AI 차별이 발생했는지 면밀히 감독

(2) 의사결정 이유의 설명 문제

XAI(e**X**plainable **AI**): 설명 가능한 AI

- 사용한 데이터 셋, 출력 오류 가능성 등의 설명을 포함할 수 있음
- 추후 법적 분쟁이 발생할 경우 재판부는 금융기관에 XAI를 활용한 설명을 요구할 수 있음

(3) 자동화된 의사결정의 문제

AI의 결론은 참고만 하고 인간이 결정하도록 인적 개입을 규정

IV. 금융법상 쟁점과 과제

6. 기타 쟁점 대응방안

(1)
고객 상담시 투명성 위험

"대화 상대가 사람인지? AI 인지?"

↓

[투명성 조치]

고객에게 생성형 AI 시스템을
사용하고 있음을 고지

ex. 생성형 AI 사용 이유, AI에 의해 생성된 내용의
품질 보증 등에 대해 게시

(2)
반경쟁 위험

"알고리즘의 묵시적 담합"

다수의 금융기관이 동일한 AI 알고리즘을 사용하는 경우

금융소비자는 선택의 여지 없이

같은 금리로 대출을 받아야 할 가능성이 있음

↓

관련 연구 필요

V. 결론

"금융영역에서 생성형 AI를 비롯한 AI의 규제 방향을 어떻게 정할 것인가?"

EU의 AI법은, 용도별 위험성의 정도에 따라 AI를 분류하고 **고위험 AI**에 규제를 집중

- 이는 규제력의 낭비를 예방하고 효율성을 추구한다는 점에서 타당함
- 우리나라 AI 법안들의 기본 규제 방향이기도 함
- 또한 생성형 AI를 비롯한 범용 AI를 따로 규율하면서 기본적으로 규제를 최소화하되 고위험 용도로 사용될 가능성도 염두에 두는 점도 참고할만 함

V. 결론

다만, EU의 AI법은 금융 분야를 고위험 AI로 명시하지 않았지만

대출, 신용평가, 보험계약 같은 세부 금융 영역에서는 개인의 평가수치가 왜곡될 경우 심각한 영향을 줄 수 있기 때문에, 이러한 경우에는 고위험 AI로 규제하는 것이 바람직함

- 나머지 금융 영역에서 AI의 활용은 최대한 자유롭게 하고 사후적으로 규제하는 방식을 취하는 것이 타당함

"지나친 규제는 금융 AI 산업의 위축을 초래할 수 있으므로
규제를 최소화하면서 유연하고 시장을 존중하는 방향으로
법적 규율이 이뤄져야 함"

토론 주제

"금융 분야에서 생성형 AI 활용 시
'법적 규제 강화'와 '자율 규제' 중
어느 규제방식이 타당할지 논하시오"

감사합니다!

Q&A

Pitch

Want to make a presentation like this one?

Start with a fully customizable template, create a beautiful deck in minutes, then easily share it with anyone.

Create a presentation (It's free)