

인공지능입문

음성 기반 금융 서비스 제공 챗봇

2024.11.05

하서휘

Contents

01	프로젝트 소개 및 목표
02	현재 진척도
02-1	알고리즘 흐름도
02-2	Llama-3 모델이 수행할 역할
02-3	Batch 기법 적용
02-4	1st Future work
02-5	RAG 기술 사용
02-6	Clova 및 Google api 사용
02-7	지식 그래프 구상
02-8	2nd Future work

01 프로젝트 소개 및 목표

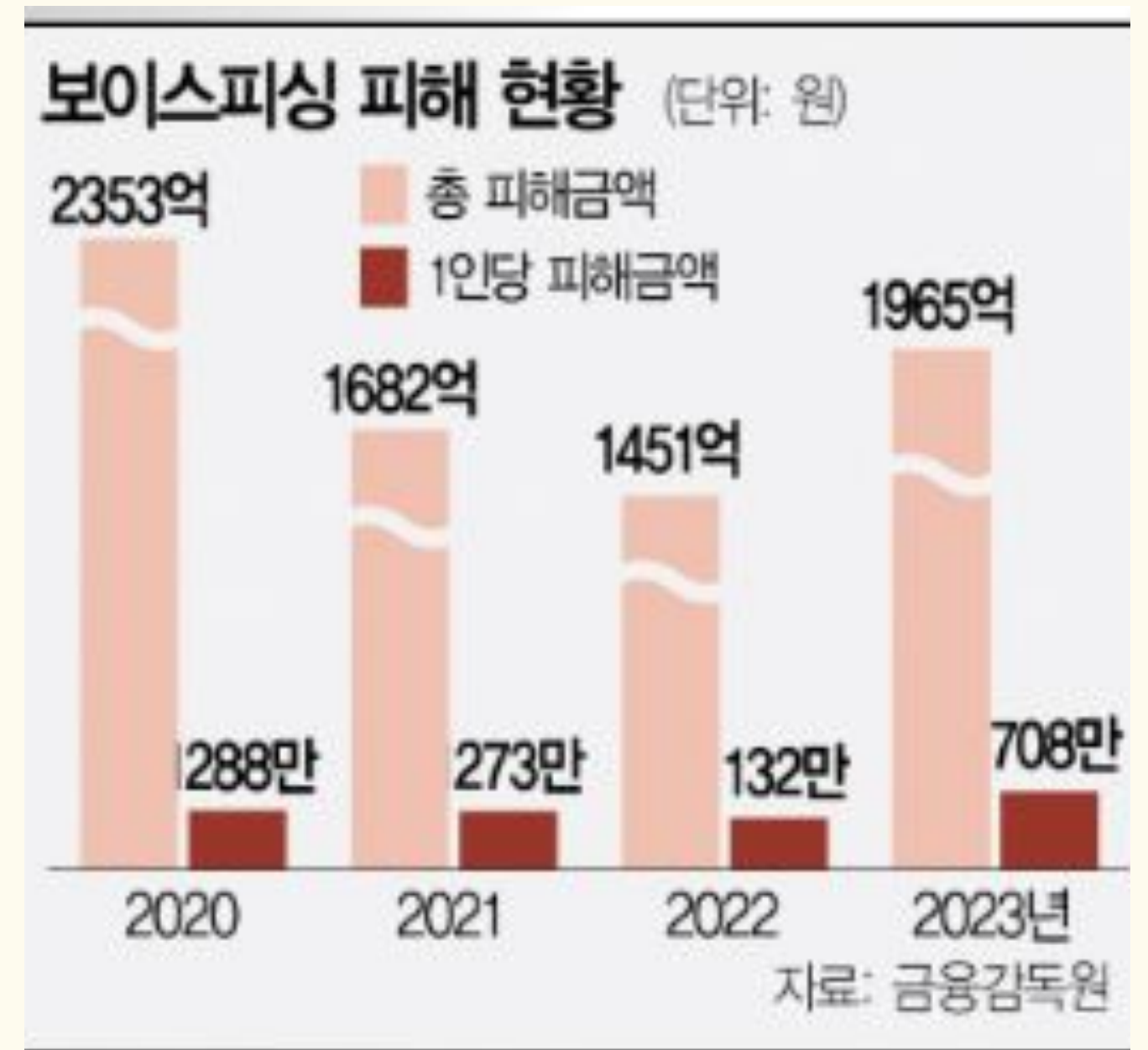
주제 소개

1. 반등하기 시작한 보이스피싱 피해 및 개인 피해금액의 급증
2. 보이스피싱 탐지 앱은 있지만, 계좌 조회 기능까지 통합된 서비스는 찾아보기 어려운 실정

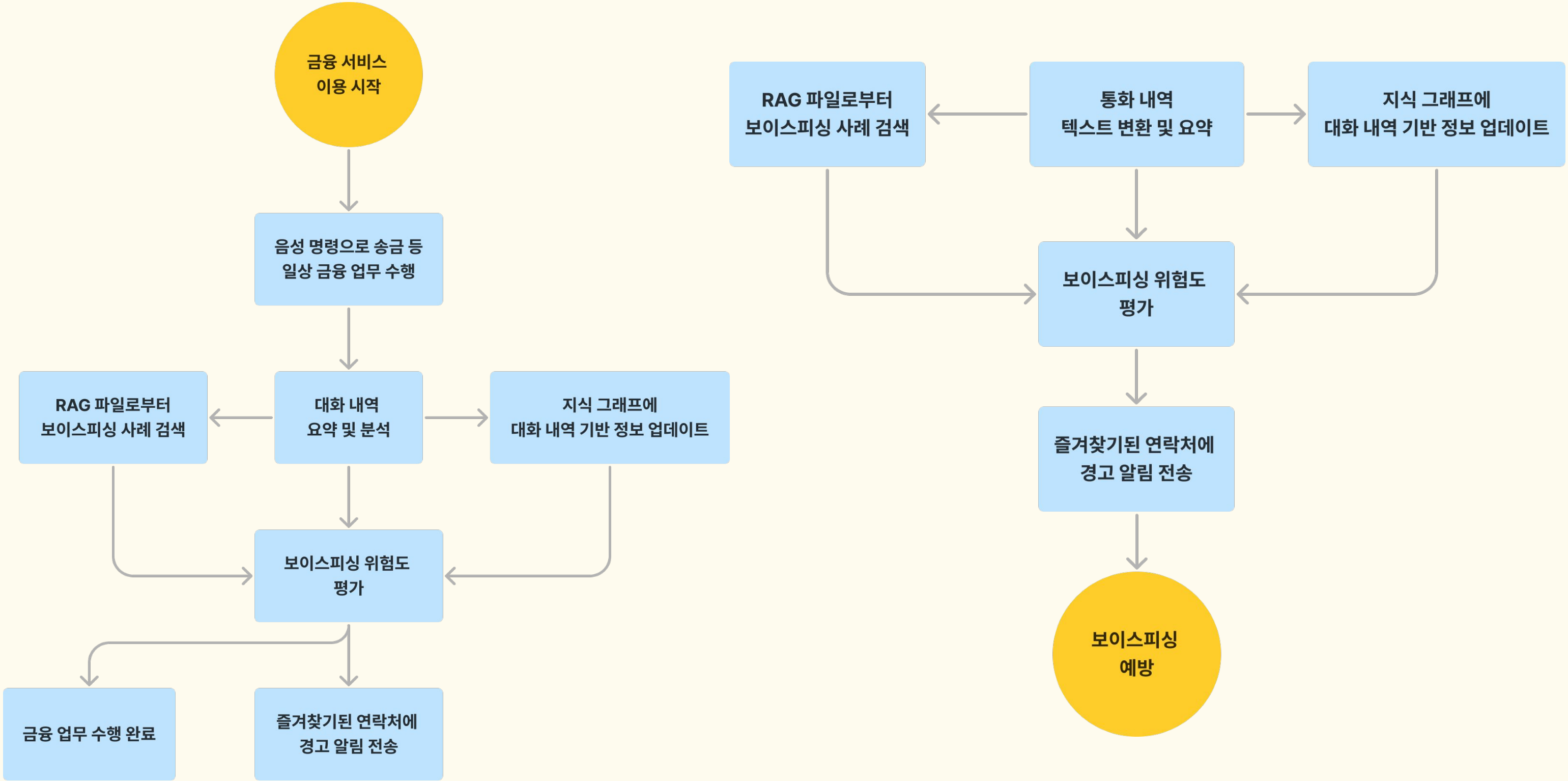
프로젝트 목표

디지털 취약 계층에게 직관적이고 접근성이 높은 음성 기반 금융 서비스를 제공

현재 상황



02-1. 현재 진척도 : 알고리즘 흐름도



02-2. 현재 진척도: Llama-3 모델이 수행할 역할

Llama-3 모델이 수행할 역할

1. LLM이 은행 업무를 제공하면서 사용자에게 유도 질문 전달 및 대화 내역을 관계식으로 요약
2. 요약된 현재 정보와 과거 내역 정보들을 토대로 보이스피싱 위험도 분석
(이름, 계좌, 송금내역은 지식 그래프에 저장되어 있다고 가정.)
3. 상대방과의 통화 내역을 관계식으로 요약 및 보이스피싱 위험도 분석
(이미 보이스피싱 사례 및 대응책이 RAG 기술로 학습되었다 가정.)

02-3. 현재 진척도: Batch 기법 적용

가상 사용 예시

```
{
  "role": "user",
  "content": "{요약된 대화 내용}. {다음 요청 사항... ex. 이런 상황인데 보이스피싱에 노출된 위험도를 알려줘.}",
},
{
  "role": "assistant",
  "context": "알겠습니다. 사용자는 보이스피싱 위험도가 높은 상황에 처해있는 것으로 보입니다.",
},
```

batch 별로 사용자1, 사용자2로 구분짓고, batch 내 user : content에 모델과의 대화 내용 또는 요약된 통화 내용을 전달할 수 있다.
이어 다음 요청 사항으로 전달한 데이터를 바탕으로 보이스피싱에 노출된 위험도를 알려달라 요청이 가능하다.

02-3. 현재 진척도: Batch 기법 적용

```
# 시스템 메시지로 대화 설정
process_user_input("처음부터 끝까지 일관되게 한국어로 대답해줘. 너는 은행 업무 전문가야.", role="system")

# 첫 번째 사용자 메시지
process_user_input("user_1", "송금을 하려고 해.")
# 첫 번째 assistant 응답
process_user_input("user_1", "송금 관련하여 어떤 도움을 드릴 수 있을까요?", role="assistant")

# 두 번째 사용자 메시지
process_user_input("user_2", "아들에게 100만원을 송금하려고 해.")
# 두 번째 assistant 응답
process_user_input("user_2", "아드님의 계좌 정보를 확인해 주시면 송금 진행을 도와드리겠습니다.", role="assistant")

# 세 번째 사용자 메시지
process_user_input("user_3", "그럼 바로 진행해줘.")

# 실시간으로 사용자 입력 받기
print("대화형 모드에 진입했습니다. 종료하려면 'exit'를 입력하세요.")
user_id = input("사용자 ID를 입력하세요: ")

while True:
    user_input = input(f"{user_id} 입력: ")
    if user_input.lower() == "exit":
        print("대화형 모드를 종료합니다.")
        break

    # 사용자 입력을 처리
    process_user_input(user_id, user_input, role="user")
```

Batch 기법 사용해 Llama 3.8B Instruct
모델에 여러 개의 명령을 한꺼번에 주고
batch 별로 모델이 output을 내도록 한다.

<- 사용예시

1. LLM이 은행 업무를 제공하면서 사용자에게 유도 질문 전달 및 대화 내역을 관계식으로 요약

"혹시 자녀분들은 다들 어떻게 지내시나요?"
"오늘은 무슨 일로 은행에 오셨나요? 혹시 특별한 거래나 송금이 있으신가요?"
"최근에 자녀분들 혹은 지인분들께 갑작스런 송금 요청을 받으신 적 있으세요?"
"요즘 전화나 메시지로 계좌 관련 안내를 받으신 적 있나요?"

```
{
  "role": "assistant",
  "content": (
    "안녕하세요! 서휘님의 금융비서 은행봇입니다! 오늘은 어떤 업무를 도와드리면 될까요?"
  )
},
{
  "role": "user",
  "content": (
    "송금을 하려고 해."
    "아들에게 100만원을 송금하려고 하는데 지금 즉시 이체해줄 수 있어?"
  )
},
```

생성답변: 송금이 필요한 경우가 이렇게 필요해지는 건가요? 😊 오늘은 당신의 가족 구성원들은 다들 잘 지내고 계신가요? 아들이 100만원을 받는 것 같으면 그 이유는 무엇입니까?

추후 개선사항:
프롬프트 수정 및 디코딩 시도를 통해 유저 친화적인 질문 생성.
이를 통해 유저로부터 유용한 정보 획득

2. 요약된 현재 정보와 과거 내역 정보들을 토대로 보이스피싱 위험도 분석 (이름, 계좌, 송금내역은 지식 그래프에 저장되어 있다고 가정.)

```
{
  "role": "system",
  "content": (
    "처음부터 끝까지 일관되게 한국어로 대답해줘."
    "너는 보이스피싱 탐지 전문가야. 사용자가 제공한 정보를 분석해 보이스피싱 여부와 대응 방안을 제시해."
    "정보를 분석해서 사용자가 보이스피싱에 노출된 위험도를 알려줘."
  )
},
{
  "role": "user",
  "content": (
    "철수는 영희를 친구로 생각한다. 철수는 10월 21일에 영희에게 100만원을 송금한 전적이 있으며"
    "10월 27일 현재 영희에게 100만원을 송금할 예정이다."
  )
},
},
```

생성답변: 보이스피싱 탐지 전문가로써, 저는 분석결과 다음과 같은 결론을 내리겠습니다.

제1단계: 정보 분석 철수와 영희의 사이에 돈을 송금한 적이 있는 것 같습니다. (10월 21일에 100만원을 송금) 10월 27일에 또다시 100만원을 송금할 예정인 것 같습니다.

제2단계: 이상 징후 확인 철수와 영희의 사이에 돈을 송금한 적이 있는 것은 일반적으로 문제가 없는 것이지만, 2번에 걸쳐 돈을 송금할 필요가 있는지 확인해야 합니다. 철수가 10월 27일에 100만원을 송금할 예정인데, 이는 이례적으로 큰 액수의 송금입니다.

제3단계: 보이스피싱 여부 확인 보이스피싱이 있는지 확인하기 위해, 저는 다음과 같은 점을 고려합니다. 철수가 10월 27일에 100만원을 송금할 예정인데, 이는 보통의 이익 관계에서는 일반적으로 일어나는 거래가 아니라는 점.....

3. 상대방과의 통화 내역을 관계식으로 요약 및 보이스피싱 위험도 분석

```
{
  "role": "system",
  "content": (
    "처음부터 끝까지 일관되게 한국어로 대답해줘."
    "너는 보이스피싱 탐지 전문가야. 사용자가 상대방과 통화한 내역을 누가/무엇을/어떻게 하였다 라는 관계식으로 요약해줘."
    "그리고 요약한 내용을 분석해서 사용자가 보이스피싱에 노출되었는지 의심되는 여부와 그 근거를 3가지만 제시해줘."
  )
},
{
  "role": "user",
  "content": (
    "택배 회사에서 하서휘에게 배송 사고가 발생했다고 연락해 본인 인증이 필요하다는 주민등록번호와 계좌 정보를 요청한다. "
    "이후 계좌에서 의심 거래가 발생했다며 경찰청 수사관과 연결해 준다. "
    "수사관은 자산 보호를 위해 지정된 계좌로 돈을 옮기라고 지시하고, 하서휘는 안내에 따라 돈을 이체한다.")
  )
}
```

생성답변:

관계식: 하서휘 (사용자) → 택배 회사 → 경찰청 수사관

요약: 택배 회사에서 하서휘에게 배송 사고가 발생했다고 연락해, 주민등록번호와 계좌 정보를 요청했다. 경찰청 수사관과 연결된 후, 수사관은 자산 보호를 위해 지정된 계좌로 돈을 옮기라고 지시하고, 하서휘는 안내에 따라 돈을 이체했다.

보이스피싱 여부 의심 3가지 지점:택배 회사에서 주민등록번호와 계좌 정보를 요청하는 것이 일반적이지 않다. 보이스피싱으로 의심할 수 있다.....

02-4. 1st Future work

1. 최대한 유용한 정보를 사용자로부터 얻어낼 수 있도록 프롬프트 보완 및 디코딩 진행
2. 3초내로 user에게 답을 return할 수 있도록 프롬프트 수정 및 디코딩 진행

02-5. RAG 기술로 실제 보이스피싱 사례 및 대응책 학습 진행

```
{
  "id": "case_001",
  "scenario": "철수는 영희에게 송금을 하려 한다. 영희가 갑작스럽게 자금이 필요하다고 해서 큰 금액을 요구한다.",
  "response": "갑작스러운 큰 금액 송금 요청이 있을 경우 상대방의 신원을 확인하고 직접 통화하여 사유를 확인해야 합니다."
},
{
  "id": "case_002",
  "scenario": "전화로 경찰을 사칭한 사람이 철수에게 전화하여 계좌번호와 비밀번호를 요구한다.",
  "response": "경찰, 은행 등 공공기관은 절대 전화로 개인 금융 정보를 요구하지 않으므로 주의가 필요합니다."
},
```

보이스피싱 사례 검색 함수

```
def search_similar_cases(user_input, top_k=3):
    user_embedding = embedding_model.encode([user_input])
    distances, indices = index.search(np.array(user_embedding), top_k)
    return [case_data[idx] for idx in indices[0]]
```

보이스피싱 관련 사례 검색 및 추가

```
similar_cases = search_similar_cases(message)
context = "\n\n".join([f"사례: {case['scenario']} 대응: {case['response']}" for case in similar_cases])
```

사용자 대화와 관련 사례를 모델 입력에 포함

```
user_history = user_conversations[user_id] + [{"role": "system", "content": context}]
texts.append(tokenizer.apply_chat_template(user_history, add_generation_prompt=True, tokenize=False))
```


02-6. 현재 진척도: Clova Speech api 및 Google text to speech api

사용

```
# 요청에 필요한 메타데이터 설정
request_body = {
    'language': 'ko-KR',

# 파일 업로드 요청
result = client.req_upload(file=r'C:\Users\STORY\Desktop\ai_code\청파동2가.wav', completion='sync')
```

안녕하 세요. 제 이 름은 하 서 휘 입니다. 송 금 서비 스를 이용하고 싶어 금융 앱을 시작했 습니다.

안녕하세요. 제 이름은 하서휘입니다. 송금 서비스를 이용하고 싶어 금융 앱을 시작했습니다.

안녕하세요. 제 이름은 하서휘입니다. 송금 서비스를 이용하고 싶어 금융 앱을 시작했습니다.

첫 번째 예시: CLOVA 실시간 인식
두 번째 예시: CLOVA 장문 인식
세 번째 예시: CLOVA 단문 인식

결론: 챗봇 기능에는 구글 단문 인식 기능 API 보다 정확도가 높은
CLOVA 단문 인식 기능 사용
통화 내역 녹음 후 텍스트 변환에는 CLOVA 장문 인식 기능 사용

02-6. 현재 진척도: Clova api 및 Google text to speech api 사용

```
# 텍스트 설정
input_text = texttospeech.SynthesisInput(text="안녕하세요, 저는 금융 서비스 제공 도우미입니다.")

# 한국어 음성 설정
voice_kor = texttospeech.VoiceSelectionParams(
    language_code="ko-KR",
    ssml_gender=texttospeech.SsmlVoiceGender.FEMALE
)

# 음성 파일을 지정한 경로에 저장 (예: c 드라이브의 tts_output 폴더)
save_path = 
```

Google Text to speech api 사용

1. 텍스트 인식 후 음성 변환
2. 한국어 음성 설정, 여성 음성 설정
3. 지정한 경로에 mp3 파일로 저장됨.

결론: 챗봇 기능에서 Llama 모델이
사용자의 명령에 따른 답변 생성 후 이를
음성으로 출력하도록 한다.

 output_korean.mp3	2024-10-14 오전 9:04	MP3 파일	30KB
---	--------------------	--------	------

02-7. 지식 그래프 기법 적용 구상

객체의 그래프화

객체 = 노드

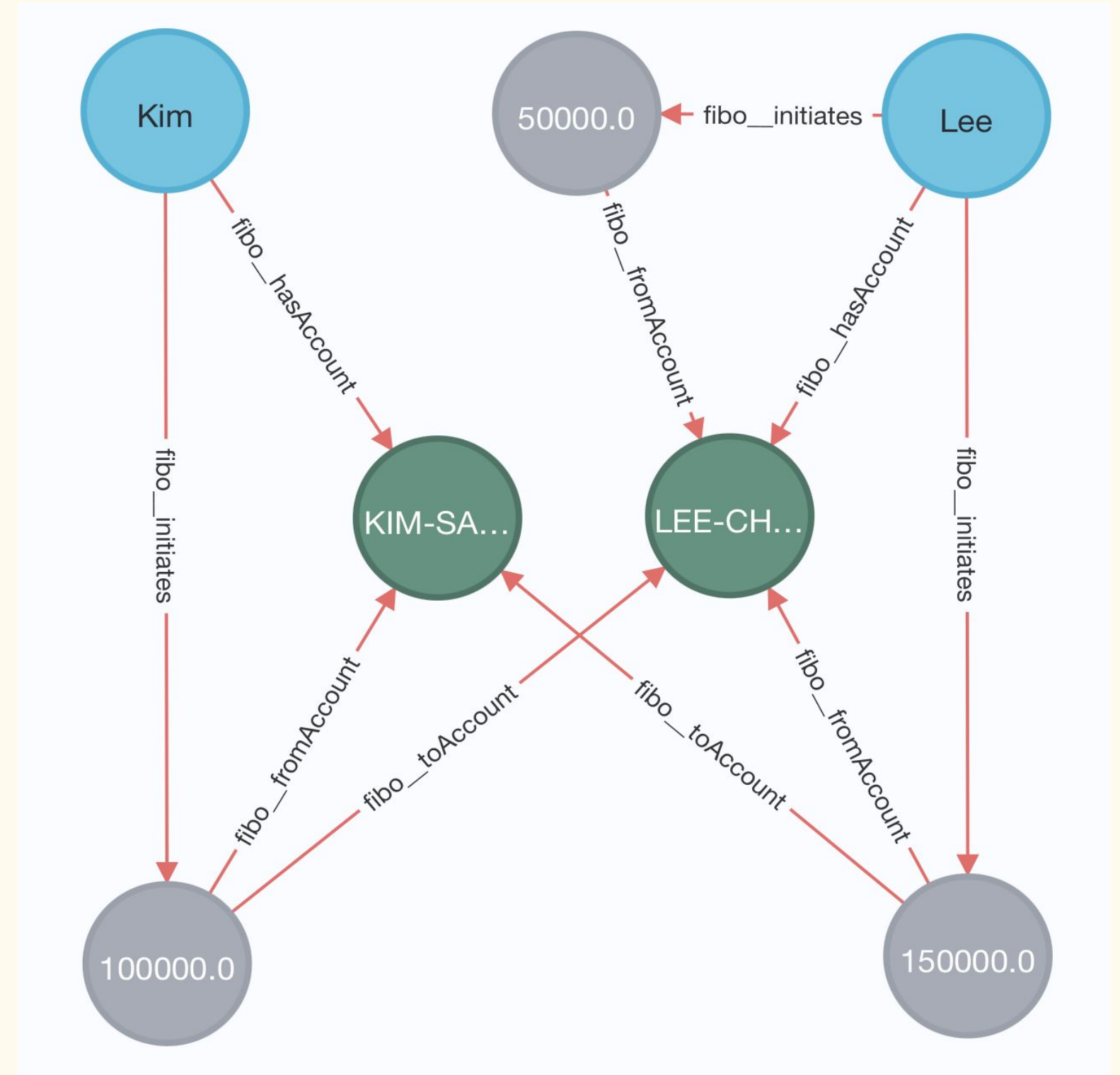
관계 = 엣지

우측 예시

김 (Kim) 과 이 (Lee) 사이에 새로운 거래 시작 내역

사용 예시

거래 당사자 간의 과거 내역을 종합적으로 불러오기
불러온 내용 바탕으로 거래의 위험도 평가



02-8. 2nd Future work

1. **csr, tts** 기능 투입해 생성된 예시 파일(통화 녹음 파일, 모델이 생성한 **text** 파일) 가져오고 내보낼 수 있도록 코드 수정 진행
2. 챗봇이 금융 서비스를 제공하도록 특정 금융 서비스 위주로 추가 학습 진행 및 **streamlit** 라이브러리 이용
3. 맥락 기억하는 챗봇에 대화 내역 및 통화 내역 요약 및 분석하도록 코드 보완 진행

03 기술 소개

∞ Meta

Llama 3

Llama-3 & RAG

다국어 지원과 뛰어난 추론 능력

모델에 최적화된 은행 업무와 관련된 명령 프롬프트를 개발하여 챗봇 구현



CLOVA Speech API & Google Text to Speech API

실시간으로 음성을 텍스트로 변환시킨 다음

생성된 답변을 사용자에게 음성으로 반환하도록 설계

neo4j

지식그래프

관련 있는 정보 조각들을 연결망으로 구성

사용자별 이전 서비스 이용 내역, 피싱 사례 데이터, 최신 금융 데이터 등을 지식 그래프 형태로 그래프 데이터베이스에서 불러오고 업데이트

인공지능입문

음성 기반 금융 서비스 제공 챗봇

감사합니다.