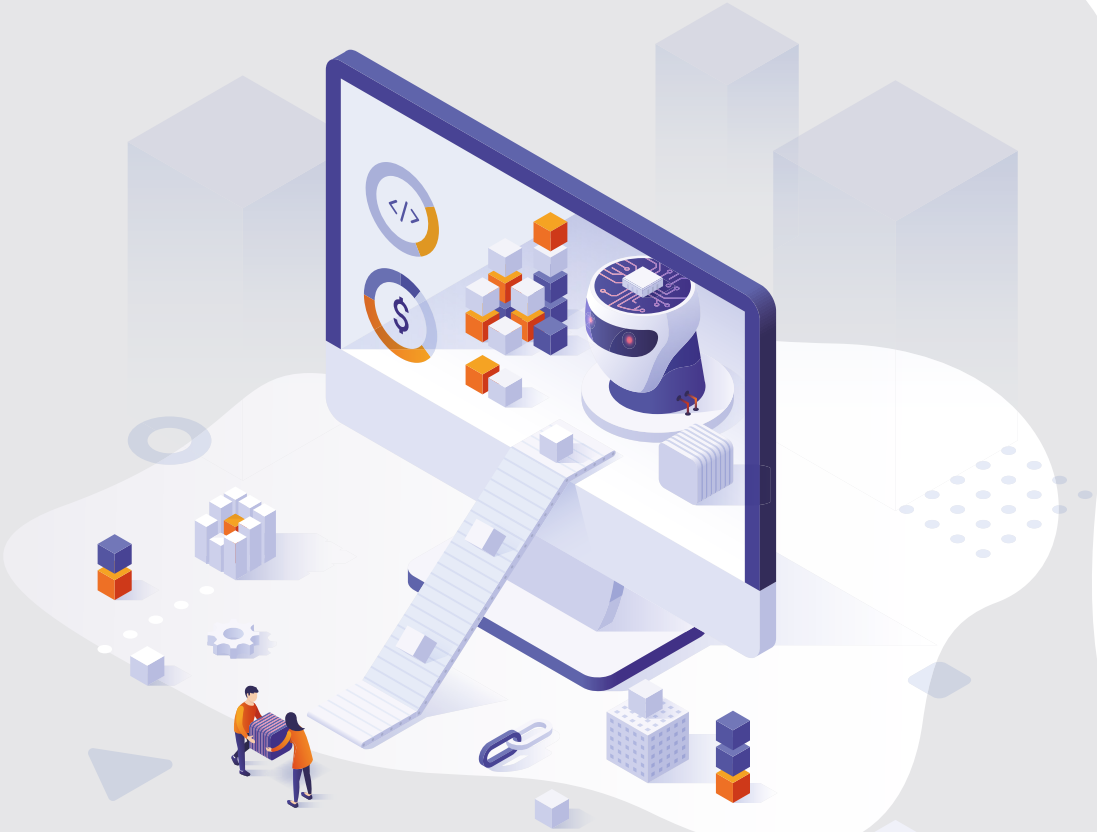
공간정보를 활용한 생성형 AI의 신뢰성 향상 및 적용방안

최형환 이지스 기술연구소 연구소장



1. 머리말

최근 생성형 AI의 발전이 다양한 분야에서 혁신을 불러일으키고 있다. GIS(공간정보시스템, Geographic Information System) 분야도 마찬가지. 생성형 AI는 데이터 활용 효율과 정확도를 크게 향상시킬 수 있는 가능성을 보여주고 있다. 다만 여기엔 여러 도전 과제와 해결할 문제가 있다.

그중 하나가 생성형 AI의 한계 중 하나인 환각(Hallucination) 현상이다. 이는 AI 모델이 실제로 존재하지 않는 정보나 사실을 만들어내는 문제를 말한다. 예를 들어, ChatGPT-3.5와 ChatGPT-4의 답변 결과를 비교해 보면, ChatGPT-3.5는 잘못된 정보와 존재하지 않는 주소를 제시하는 반면, ChatGPT-4은 인터넷 검색 결과를 기반으로 더 정확한 답변을 제공한다. 그러나 잘못된 위치 정보를 포함하는 문제가 여전히 존재한다.

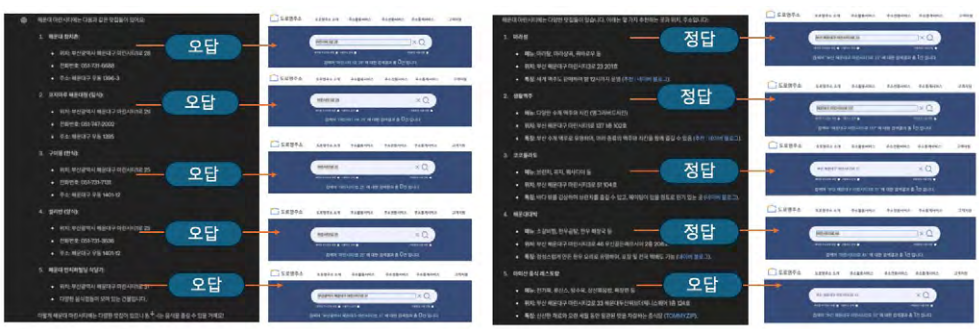
이번 원고에선 이지스 기술연구소에서 개발한 '디지털 어스 기반 공간정보 클라우드 플랫폼(www.egiscloud.com)'과 생성형 AI를 융합하는 과정에서 알게 된, 다양한 지식을 공유하고자 한다. 특히, RAG(Retrieval Augmented Generation) 모델을 활용해 AI 답변의 정확도를 높이고, 기존에 답변하지 못했던 질의에 대한 해결 방안을 모색한다. 또한, 생성형 AI를 도입할 때 주의해야 할 보안 및 비용 문제에 대해서도 논의하고자 한다.

2. 공간정보를 활용한 환각 현상 해결 방법

2.1 위치 기반 질의 환각

아래 [그림 1]은 "해운대 마린시티 맛집 정보를 알려달라"는 질문에 대해 ChatGPT-3.5와 ChatGPT-4o가 각각 내놓은 답변이다. ChatGPT-3.5의 경우 맛집 명칭이 사실과 다르고, 제시된 주소인 '마린시티 1로 25'와 '마린시티 1로 31' 또한 새주소 공식 사이트에 존재하지 않는다. 가장 성능이 좋다는 ChatGPT-4o의 답변은 그나마 정확한 편인데, 인터넷 검색 결과를 바탕으로 답변하기 때문이다. 하지만 마지막 답변인 '아미산 중식 레스토랑'의 위치가 다른 곳에 있다. 웹 사이트 검색 기반 답변이기 때문에, 검색한 사이트에 잘못된 정보가 있는 경우 그 신뢰성이 떨어진다.

이렇게 답변에 신뢰성이 떨어지는 이유는 실제로 존재하지 않는 정보나 사실을 만들어내는 환각(Hallucination) 현상 때문이다. 이는 특히 텍스트 생성 모델에서 두드러지게 나타난다.



[그림 1] 맛집 관련 질문에 대한 ChatGPT-3.5(왼쪽)와 ChatGPT-4o(오른쪽)의 답변

2.2 환각이 발생하는 이유와 해결법

생성형 AI의 환각 현상은 다음과 같은 이유로 발생할 수 있다.

- **제한된 훈련 데이터**: AI 모델이 학습에 사용한 데이터가 불완전하거나 특정 주제에 대한 정보가 부족한 경우, 모델은 그 간극을 메우기 위해 가상의 정보를 생성해낼 수 있다.
- **확률적 본성**: 생성형 AI 모델은 다음에 나올 단어를 확률적으로 예측하는 방식으로 작동한다. 이 과정에서 잘못된 단어를 선택할 수 있으며, 이는 결국 문장의 일관성을 해칠 수 있다.
- **문맥 이해 부족**: AI 모델이 문맥을 완벽히 이해하지 못하거나, 문맥을 오해할 경우 잘못된 정보를 생성할 수 있다. 이는 특히 복잡한 문장 구조나 주제를 다룰 때 빈번하게 발생한다.
- **훈련 데이터 편향**: 훈련 데이터가 특정 편향을 가지고 있거나 불균형할 경우, AI 모델은 편향된 데이터를 바탕으로 잘못된 결론을 도출할 수 있다.

환각 현상을 완화하기 위해선 다음과 같은 접근법이 필요하다.

1) **데이터 품질 향상**: 더 많은 양질의 데이터를 사용해 모델을 학습시키고, 가능한 한 많은 시나리오를 포함시키는 것이 중요하다.
2) **모델 개선**: 더 나은 알고리즘과 모델 구조를 통해 AI 문맥 이해 능력을 향상시킬 수 있다.
3) **인간 검토**: AI가 생성한 텍스트를 사람의 검토를 통해 확인하고 수정하는 과정이 필요하다.
4) **피드백 루프**: AI 시스템이 사용자의 피드백을 반영해 지속적으로 개선될 수 있도록, 피드백 루프를 구축하는 것이 중요하다.

다만 이러한 해결법은 생성형 AI 모델 자체를 개선하는 방법이기에, 오픈AI(OpenAI), 구글(Google)처럼 LLM(거대언어모델, Large Language Model)을 만드는 기업이 고려할 사항이다. 즉 생성형 AI를 응용하는 개발자 혹은 활용 기업 입장에선 고려 대상이 아니라는 뜻이다.

LLM 모델을 활용하는 입장에서, 이러한 문제를 해결하기 위해 정확한 정보를 기반으로 답변하는 기술이 RAG(Retrival Augmented Generation) 모델이다. RAG는 생성형 AI의 환각 문제를 해결하고, 정보의 정확성을 높이기 위한 중요한 기술로 자리 잡고 있다.

2.3 위치 정보 활용 정확도 향상

RAG 모델은 생성형 AI와 정보검색 시스템을 결합한 프레임워크다. 생성된 응답의 정확성을 높이기 위해 외부 데이터베이스나 지식 그래프에서 관련 정보를 검색하고, 검색 엔진이나 데이터베이스 쿼리를 통해 추가적인 정보를 수집한다. RAG 모델의 작동방식은 다음과 같다.

질의 처리: 사용자 질문이 입력되면, RAG 모델은 질문을 처리해 필요한 정보의 유형을 파악한다.

↓

정보 검색: 모델은 질문과 관련된 정보를 외부 데이터 소스에서 검색한다. 여기에는 웹 페이지, 데이터베이스, 문서 등이 포함될 수 있다.

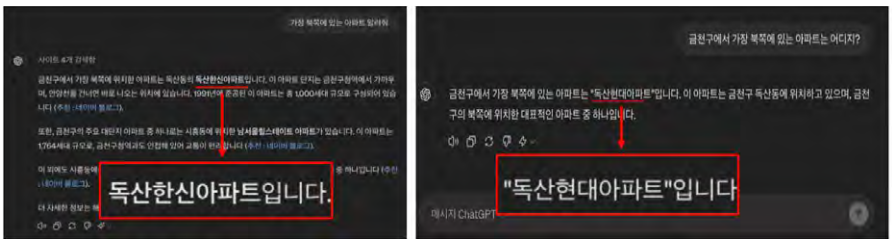
↓

응답 생성: 검색된 정보를 바탕으로, 모델은 초기 응답을 생성한다.

↓

응답 보강: 최종 응답을 생성하기 위해 검색된 정보를 사용해 초기 응답을 보강한다. 이 과정에서 정보의 정확성과 관련성을 높인다.

또 하나의 예를 들어보자. 먼저 [그림 2]와 같이 "금천구에서 가장 북쪽에 있는 아파트는 어디지?"라는 질문에 ChatGPT-3.5와 ChatGPT-4o 모델 모두 실



[그림 2] ChatGPT-4o 답변(왼쪽)과 ChatGPT-3.5 답변(오른쪽)

제와 상관없는 잘못된 답변을 한다.

이제 데이터를 사용해서 정확한 답변을 유도하는 과정을 살펴본다. 우선 data.go.kr에 공개된 '서울시 금천구 공동주택 현황 20231110.csv'데이터를 다운받는다. 이후 북쪽이라는 질문에 답변 가능하도록 주소를 기반으로 경위도 좌표 정보를 추가한다.

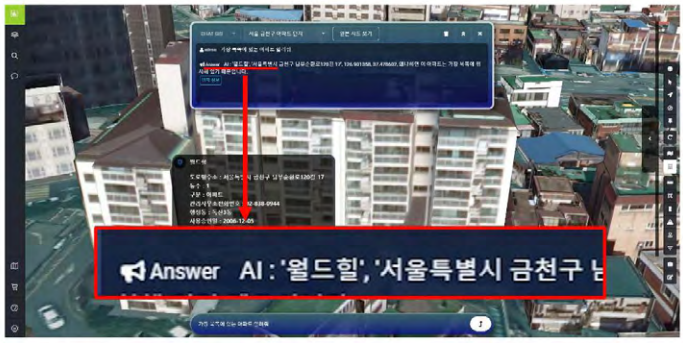
이제 ChatGPT에게 "주어진 엑셀 파일 기반으로 답변하라"는 지시어를 주고 동일한 질문을 하면, [그림 4]와 같은 답변을 제공한다.

여기서 놀라운 점은, ChatGPT가 '엑셀파일의 구분자와 데이터를 기반으로 어떤 분석을 해야 하는지'를 스스로 인지한다는 사실이다. 실제 모델 내부에선 어떤 일이 일어날까. 구체적인 답변 과정은 [그림 5]와 같다.

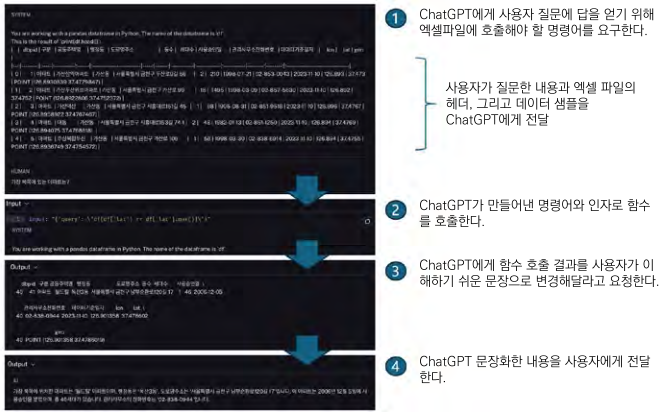
추가된 좌표

구분	공동주택명	행정동	도로명주소	동수	세대수	사용승인일	관리사무소전화번호	데이터기준일자	lon	lat
아파트	가산삼익아파트	가산동	서울특별시 금천구 두산로9길 56	2	210	1998-07-21	02-853-0043	2023-11-10	126.8930839	37.4729847
아파트	가산두산위브아파트	가산동	서울특별시 금천구 가산로 99	18	1495	1998-03-09	02-857-5630	2023-11-10	126.8922806	37.4752372
아파트	가산덕산	가산동	서울특별시 금천구 시흥대로151길 45	1	98	1995-08-31	02-851-9518	2023-11-10	126.8958922	37.4767467
아파트	대동	가산동	서울특별시 금천구 시흥대로153길 74-1	2	48	1982-01-13	02-851-1250	2023-11-10	126.894075	37.4768618
아파트	주삼복합두산	가산동	서울특별시 금천구 가산로 106	1	56	1998-03-30	02-838-6914	2023-11-10	126.8936749	37.4754572

[그림 3] 주소를 기반으로 경위도 좌표 정보를 추가한다.



[그림 4] RAG 모델을 적용한 답변



[그림 5] RAG 모델 적용 과정

[그림 5]에서 우리는 '엑셀 데이터에 기반한 RAG 모델'이 입력된 질문에 정확하게 답변하는 것은 물론, 공간정보를 추가하면 '기존에 답하지 못했던 다양한 질의에 답변이 가능'하다는 것을 알 수 있다.

3. 공간정보를 활용한 생성형 AI 답변 능력 향상

3.1 RAG에 2D GIS(SHP) 정보를 활용

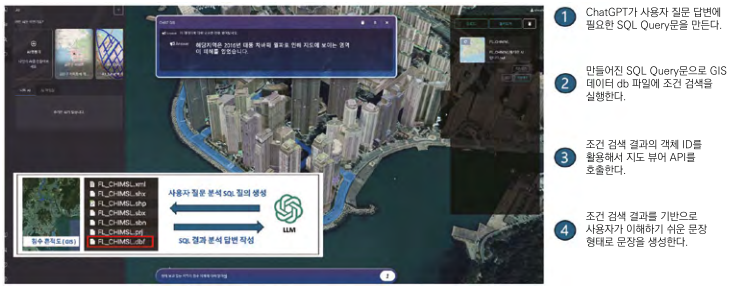
구글을 비롯해 전 세계적으로 공간정보 분야에 생성형 AI를 도입하려는 다양한 시도가 이뤄지고 있다. 이를 통해 전문가 영역이었던 GIS 데이터가 일반인에게도 좀 더 쉽게 활용될 수 있을 것으로 기대된다.

예를 들어, 침수흔적 GIS 데이터를 활용한 생성형 AI가 "지금 보고 있는 지역의 침수 이유에 대해 알려줘"라는 질문을 받았다고 하자. [그림 6]과 같이 생성형 AI는 "2016년 태풍 차바 때 월파 때문에 발생한 침수"라는 답변을 제공할 수 있다.

이는 기존의 복잡한 명령어, 예를 들어 'select * from flchimsl where lat betwin 34 and 38.0 and lat betwin 126.0 and 130.0'와 같은 쿼리를 작성하지 않아도 사용자들이 다양한 질의를 할 수 있게 해준다.

3.2 RAG에 3D GIS 정보를 활용

RAG 모델 중 API 연계 부분이 있다. ChatGPT에게 특정 API에 대한 스펙을 알려주면, 사용자 질의에 대한 답변에 필요한 경우 해당 API에 대한 호출문장을 생성해 실행하고, 리턴값을 활용해 답변하는 것이다. 이 기능을 활용하면 "주변 전월세 정보 알려줘"라는 질문에 답하기 위해, 3D 지도 API를 호출해 [그림 7]과 같이 제시할 수 있다. 또한 공간 분석 API와 연동하면, "한 변에 있으면서 주변에 초·중·고등학교가 있는 아파트를 찾아줘" 와 같이 기존 ChatGPT가 대답할 수 없는 질문에 대한 답변도 가능하다[그림 8].



[그림 6] ChatGPT를 활용한 대화형 질의

[그림 7] 전월세 검색

[그림 8] 반경 검색 연동 아파트 검색

4. ChatGPT 연계 활용 시 주의점

4.1 보안

성능 향상을 위해 RAG 모델을 도입할 경우, 보안을 주의해야 한다. 바로 미세조정(Fine-tuning)을 적용할 때다. 미세조정은 이미 학습된 LLM에 새로운 데이터를 추가 학습시켜 특정 작업이나 도메인에 최적화하는 과정이다. 이를 통해 모델의 성능을 더욱 향상시킬 수 있다. 특히 가지고 있는 데이터를 질의응답 형태로 구축해 모델의 답변 성능을 향상시키기 위해 미세조정을 사용한다.

하지만, 미세조정 과정에서 몇 가지 주의해야 할 사항이 있다. 미세조정 과정에서 데이터가 LLM 회사 서버로 이전되는 상황이 생기는 것이다. 이는 보안 및 개인정보 보호 측면에서 문제가 될 수 있다. 특히, 공간정보와 같은 민감한 데이터는 해외 서버로 이전이 불가능한 경우가 많기 때문에, 이러한 보안 사항을 유의해 미세조정을 진행해야 한다.

4.2 API 사용 비용

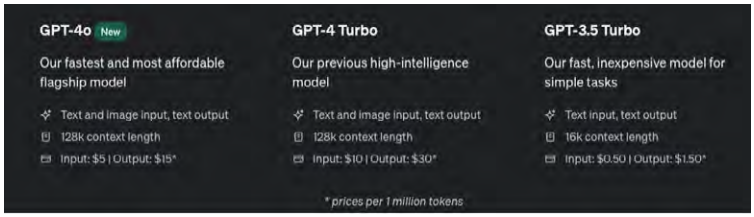
기본적으로 생성형 AI를 업무에 도입할 때, 질문과 답변의 글자 수에 따라 API 과금이 발생한다. 만약 RAG 모델 기반으로 생성형 AI를 도입하면, 사용자 질의에 따라 내부적으로 여러 번의 ChatGPT 호출이 발생할 수밖에 없다. 결국 한 번의 사용자 질문과 답변에 대해 기존보다 3~10배 이상 과금이 발생할 수 있다는 뜻이다. 따라서 모델 도입에 따른 API 비용도 신경 써야 한다. 특히 ChatGPT-4의 경우 ChatGPT-3.5에 비해 RAG 모델 활용 시 효과가 좋기는 하지만, API 호출 비용이 약 20배 정도 차이나기 때문에 신중하게 선택해야 한다.

5. 맺음말

지금까지 생성형 AI를 공간정보 분야에 적용함으로써 발생하는 다양한 문제와 그 해결 방안을 살펴봤다. 그중에서도, 생성형 AI 모델의 환각 현상을 줄이고 답변 정확성을 높이기 위해 RAG 모델을 활용하는 방법을 다뤘다. RAG 모델은 외부 데이터베이스와의 연계를 통해 좀 더 정확한 정보를 제공할 수 있게 하며, 이를 통해 사용자는 복잡한 쿼리 없이도 다양한 질의에 대한 정확한 답변을 받을 수 있다.

또한, 공간정보를 활용한 생성형 AI의 적용 사례를 통해 그 가능성을 확인했으며, 이 과정에서 주의해야 할 보안 및 비용 문제도 함께 살폈다. 특히 미세조정 과정에서의 보안 이슈와 API 호출 비용을 고려해 신중하게 접근해야 함을 강조했다.

앞으로 생성형 AI와 공간정보의 융합은 더욱 활발히 진행될 것이며, 이를 통해 GIS 데이터 활용이 일반인에게 좀 더 쉽게 접근가능해질 것이다. 이번 원고가 이러한 발전에 기여하길 기대하며, 지속적인 연구와 개선이 필요함을 다시 한번 강조한다.



[그림 9] ChatGPT 모델별 가격(오픈AI 홈페이지 2024.5.23. 기준)