전력산업에서 대규모언어모델(LLM) 활용 방향에 관한 연구

김은진, 이정숙*, 이수미**, 신용태***

숭실대학교

sonaflux30@soongsil.ac.kr, *jungsuk2023@soongsil.ac.kr, **leesumi@soongsil.ac.kr, ***shin@soongsil.ac.kr

A Study on the Direction of Large Language Model(LLM) Utilization in the Domestic Power Industry

Eunjin Kim, Jungsuk Lee*, Sumi Lee**, Yongtae Shin***

Soongsil Univ.

요 약

본 연구의 목적은 국내 전력산업을 대상으로 LLM을 활용하기 위한 대외적 제약을 세밀히 검토하고, 이를 극복하거나 우회하는 방식으로 업무에 적용하기 위한 전략을 제시하는 것이다. 본 연구는 LLM과 관련된 문헌 연구를 통해 외부 환경을 분석하고, 이를 토대로 전력산업에서 LLM의 활용 방향성을 도출할 것이다. 이를 통해 국내 전력산업에 특화된 LLM 활용에 대한 향후 구체적인 실행계획을 마련하고, 전력산업의 미래 발전에 기여할 것으로 기대한다.

Ⅰ. 서 론

전력산업에서도 벨류체인에 특화된 서비스를 개발하고 사전학습된 Foundation Model의 기능 활용을 통해 LLM을 업무 보조 도구로써 더욱 편리하고 효율적인 활용방안 모색하고 있다. 전력산업은 특성상 전 산업 및 국민의 생존에 직접적으로 관련되는 기반 산업으로서, 경제적으로 비탄력적이고 필수재로서의 특징을 가진다. 따라서 전력산업은 타 산업대비 국가적으로 영향력이 크며, 해당 산업에 LLM의 활용 방향성과 거시적 전략을 확립함으로써 신기술을 활용한 전력산업의 효율화를 도모하여 국가적 효익을 극대화하고자 한다.

Ⅱ. 본 론

대규모언어모델(이하 LLM)은 자연어를 학습하여 실제 인간언어와 유사한 문장을 생성하기 위한 언어모델로 점차 규모가 커지며 초거대 AI로 진화했다. LLM은 순차 데이터의 컨텍스트를 학습할 수 있는 신경망인 Transformer 모델을 통해 비약적 성능 발전을 이뤘는데, 최근 방대한 파라미터 크기와 데이터 학습을 통한 성능면에서 '초거대 언어모델'로 불리고 있다.[1] Transformer 모델은 구글에서 2017년 Transformer AI를 발표하면서 혁신을 주도하였는데, 美 스탠퍼드대는 2021년 Transformer를 Foundation Model로 명명하면서, Foundation Model이 AI 패러다임 견인할 것을 예측했다[2][3].

LLM은 자연어 처리 작업에서 높은 성능을 발휘하는데, 사전 학습된 자료를 기반으로 문맥을 이해하고 적절한 답변을 제공하는 언어적 작업이 가능하다. 산업에서는 주로 LLM을 위주로 활용하는데, 초거대 AI의 언어적 학습능력을 바탕으로 기업의 내부데이터를 반영하고 이를 통해 특화서비스를 발굴중이다[4].

산업 영역별 특화서비스 개발은 2가지 방식으로 수행하는데 ① 초거대 AI 플랫폼(Foundation Model, 일반지식)에 특화 전문지식을 추가로 학습(Fine-tuning)시키는 방식과 ② 특화서비스별로 경량화된 초거대 AI 플랫폼에 일반지식+전문지식을 구축·활용하는 방식의 2가지 큰 흐름으로 발전중이다. ① 방식은 전문분야 지식뿐만 아니라 일반지식으로 확장성 등에 강점이 있고, ② 방식은 해당 전문 영역에서 비용 효율적 성능 달성, 보안 문제 측면 등에서 강점이 있다[4]. 이런 산업에서의 활용을 챗GPT와 전력산업에의 사례를 들어 개념적으로 표현하면 [그림 1]과 같다.

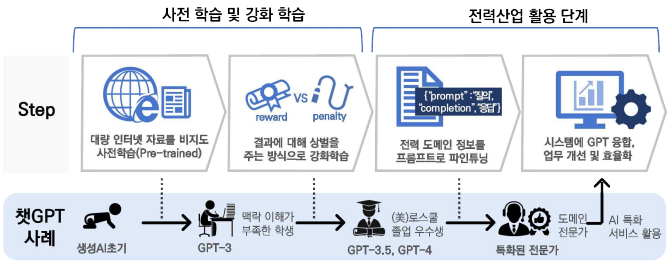

그림 1. 초거대 AI에 파인튜닝을 적용한 서비스 확대 방안
Fig. 1. Expansion of services applying fine tuning to hyperscale AI

국내 전력산업의 벨류체인은 발전-송전-배전-영업에 이르는 전통적 본원적 활동과 전략기획-경영관리-ICT 및 R&D 등 가치창출에 간접 기여하는 지원적 활동으로 구분할 수 있다[5]. 벨류체인의 세부 활동들 향후 LLM을 활용한 전력 특화서비스로 발굴될 수 있다.

발전분야의 약 40%를 차지하는 대기업를 제외하고 국내 전력산업은 공공기관 위주의 반독점적 형태로 운영되고 있다[6]. 또한 공공기관에서 추진하는 정보화 사업의 경우, 「전자정부법」과 대표 행정규칙인 「행정기관 및 공공기관 정보시스템 구축·운영 지침」을 따라야 하며, 중앙행정부처와 동일한 수준으로 관련 규정 준수에 대한 책임과 의무를 진다. 따라서 국내 전력산업은 LLM 활용과 관련해서는 보안이슈, 정부 정책 및 관련 제도, 결과물의 신뢰성 등 종합적 측면을 고려해야 한다.

1. 보안이슈

1.1. 질의를 통한 민감정보 유출 우려

챗GPT, Gemini 하이퍼클로버X 등 범용 LLM 서비스는 입력된 질문기록을 저장되어 AI 개선에 활용될 수 있으므로 불특정 다수에게 질의를 통해 입력한 민감정보 유출 가능성이 존재한다[7]. 때문에 삼성전자, 포스코, 애플 등 국내외 일부 기업은 ChatGPT 이용금지 및 제한적 사용 방침으로

하고 있다[8]. 또한, ChatGPT 사칭 앱과 플러그인을 통한 계정 탈취, 악성 프로그램 설치 등 해킹 증가 추세로, 이에 대한 대비책이 시급하다.

1.2. 배타적 환경을 갖는 기업형 범용 LLM 서비스의 한계

마이크로소프트은 클라우드 애저(Azure)내에서 OpenAI 서비스를, 구글은 구글 클라우드내에서 버텍스 AI(Vertex AI)를, 아마존은 클라우드 AWS를 활용한 베드록(Bedrock)을 통해서 기업형 범용 LLM 서비스를 제공하고 있다. 안전을 보장하는 클라우드 기반의 배타적 환경을 제공하고 있으므로 정보유출의 가능성은 낮다고 할 수 있으나, 공공에서 사용할 수 있도록 보안인증을 받은 클라우드 서비스(SaaS, PaaS, IaaS)가 없어 전력산업에서도 단기간 내 사용을 기대하기는 곤란하다.

1.3. 내부설치 방식을 통한 보안이슈를 해소한 경량형 LLM

이러한 보안이슈 틈새시장 기회로 활용하고자 국내 AI 서비스 중소 업체들은 LLM의 상대적 경량화를 통해 비용 효율성을 높인 자체 모델을 개발하거나 및 타사 기반모델을 보완하여 상업화를 추진하면서 기업 내부에 구축가능한 오프레미스형 또는 프라이빗 클라우드형을 판매하고 있다[9]. 이는 전력산업에서 보안이슈를 해소를 위한 대안이 될 수 있다.

2. 정부 정책 및 제도 한계

2.1. 전력산업에서 활용 가능한 범용 LLM 부재

앞서 언급한 바와 같이 범용 LLM 서비스 중 정부의 인증을 받은 클라우드 서비스는 없다[10]. 하지만 중앙행정부처 및 공공기관은 「클라우드 컴퓨팅법」(2015.3, 국내 클라우드 산업을 육성하고 안전한 클라우드 환경 조성을 위한 법률)에 의해 CSAP(Cloud Security Assurance Program, 안전·신뢰성이 검증된 민간 클라우드를 인증하는 제도)을 받은 클라우드 서비스만을 이용해야 한다[11]. 따라서 사실상 전력산업에서는 정부 인증을 받아서 공식적으로 사용가능한 범용 LLM은 부재하다고 볼 수있다. 주요 기업별 범용 LLM의 보안 및 제도를 비교하면 [표 1]과 같다.

2.2. 활용에 제약이 없고 기업에 특화된 경량형 LLM

챗GPT(GPT3.5)의 파라미터는 1,750억개, Gemini는 1조개, 하이퍼클로버X는 2,040억개 등 막대한 연산력을 갖춘 범용 LLM의 파라미터수에 비교하여, 70억개(7B)~500억개(50B)개로 줄인 경량형 LLM(이하 sLLM)이 2023년 하반기 전후로 퍼블릭 클라우드형 뿐만 아니라 온프레미스, 프라이빗 클라우드형으로도 출시되었다. 국내 주요 중소업체에서 개발한 sLLM을 정리하면 [표 2]와 같다.

표 1. 주요 기업별 범용 LLM 보안 및 제도 비교
Table 1. Comparison of universal LLM security and policy by major companies

주요 기업	언어모델	범용 LLM 보안 및 제도 현황 (●적합, ◑ 가능성있음, ○부적합)	
OpenAI (美)	GPT 3.5, GPT4	· 보안 별도 배타적 환경 미제공	○ 부적합
		· 제도 미인증, 공공 활용 불가 - 한국을 타겟팅한 인증 계획 없음	○ 부적합
Microsoft Azure (美)	GPT 3.5, GPT4	· 보안 기업 전용 환경 가능	● 적합
		· 제도 미인증, 공공 활용 불가 - CSAP 인증 취득 준비 중	◑ 인증시도
Google (美)	Gemini	· 보안 기업 전용 환경 가능	● 적합
		· 제도 미인증, 공공 활용 불가 - 한국을 타겟팅한 인증 계획 없음	○ 부적합
NAVER (韓)	하이퍼 클로바X	· 보안 기업 전용 환경 가능	● 적합
		· 제도 미인증, 공공 활용 불가 - CSAP 인증 취득 준비 중	◑ 인증시도

표 2. 국내 주요 중소업체가 개발한 경량형 LLM
Table 2. sLLMs developed by major domestic small and medium-sized companies

주요 기업	언어 모델	제공 형태
솔트룩스	루시아GPT	SaaS, 내부구축형
마음AI	MAAL1	SaaS, 내부구축형
코난테크놀로지	코난LLM	SaaS, 내부구축형
포티투마루	LLM42	내부구축형
업스테이지	Solar	SaaS, 내부구축형
스캐터랩	PingPong-1	SaaS

sLLM은 보안이슈에 따른 대안뿐만 아니라 내부구축 가능한 일종의 패키지 형태이므로 특별한 제약이 없다. sLLM은 기업에 요구하는 기능만 설계한 경량화 버전의 LLM으로 미세조정(Fine-Tuning)으로 정확도를 높일 수 있다. 따라서 산업에서는 범용 LLM처럼 모든 것에 정통한 AI가 아니라 특화된 도메인 업무를 잘하는 AI가 필요하다는 점에서 sLLM은 범용 LLM 보다 적합하다. 또한 규모가 작기 때문에 개발·운영비를 상대적으로 크게 절감할 수 있다[12].

3. 결과물의 신뢰성

3.1. 최신성, 정확성 등 한계 존재, 결과 책임 소재 불분명

범용 LLM은 답변을 생성하고 정확성과는 별개로 문법적으로만 완전한 문장을 구현, 편향가능성, 환각현상 및 실시간 정보제공이 불가능한 문제가 있다. OpenAI는 챗GPT '이용약관'에도 면책조항에 서비스의 중단, 콘텐츠의 정확성, 무결성, 안정성 등을 보증하지 않고 사용자에게 책임 부과하고 있다. 따라서 향후 이용 피해가 발생하는 경우, 충분한 원인과 책임 파악, 피해 구제가 곤란할 수 있다. 따라서 LLM의 결과물에 대한 신뢰성을 확보하려면, 범용 LLM를 활용하기 보다는 업무 범위를 한정하여 RAG(검색증강)와 sLLM을 활용을 대안으로 검토해야 한다.

전력산업에서 초거대 AI 및 범용 LLM을 활용하기 위해 공공부문 도입에 직면하는 보안이슈, 정책·제도 미흡, 불완전 신뢰성 등 외부환경에 따른 제약적 상황에 대한 고려가 필요하다. 외부 제약적 환경에서는, 여건에 맞는 단계적 확대 방안 모색이 합리적이다. 따라서 제약과 무관한 과제는 즉시 실행하고, 제약과 관련된 과제는 제약이 해소되는 여건에 맞게 추진하는 단계적 접근이 필요하다. 단기적으로 데이터 민감도 낮은 분야 중심으로 가능성을 검증하고 역량을 축적한다. 중기적으로 sLLM 및 정부인증을 받은 범용 LLM에 대해 전력 특화 서비스를 본격 추진한다. 전력산업에서 LLM 활용 방향을 정리하면 [그림 3]과 같다.

그림 3. 국내 전력산업의 LLM 활용 방향
Fig. 3. Direction of LLM utilization in the domestic electric power industry

Ⅲ. 결 론

본 논문에서는 국내 전력산업을 대상으로 LLM을 활용하기 위한 대외적 제약을 세밀히 검토하고, 이를 토대로 전력산업에서 LLM의 활용 방향성을 도출하였다. 해당 방향성을 기반으로 국내 전력산업에 특화된 LLM 활용에 대한 구체적인 전력특화 과제를 향후 도출하고 즉시-단기-중기 실행계획을 마련할 것이다. 또한 LLM의 시장동향, 기술성숙도 및 정부정

책 등 제반 여건을 지속적으로 모니터링하여 단계적 업무 적용을 추진해야 한다.

본 논문을 통해 산업 영향력이 큰 전력산업에 업무 효율성 제고 및 생산성의 도구로서 LLM의 활용 방향성과 거시적 전략을 확립하였다. 후속 연구로 현장 실무자들의 수요를 감안하여 상세 과제를 도출하고, 직접적 이행을 통해 신기술을 활용한 전력산업 효율화를 도모하여 국가적 효익의 극대화를 기대한다.

참 고 문 헌

[1] 소프트웨어정책연구소, “초거대 언어모델의 부상과 주요 이슈”, *SPRI ISSUE REPORT*, IS-158, pp. 4, Feb. 2023.

[2] Vaswani, Ashish, et al. “Attention is all you need.”, *Advances in neural information processing systems* 30, 2017.

[3] Bommasani, Rishi, et al. “On the opportunities and risks of foundation models.” arXiv preprint arXiv:2108.07258, 2021.

[4] 과학기술정보통신부, “초거대 AI 경쟁력 강화 방안”, Apr. 2023.

[5] 허준혁, “글로벌 유틸리티 Value Chain 별 수익성 및 사업전략 분석”, *전기저널*, pp. 38-51, 2020.

[6] 한국전력공사 전력통계월보, 제544호, Feb. 2024 (https://home.kepco.co.kr/kepco/KO/ntcob/list.do?boardCd=BRD_000097&menuCd=FN05030101)

[7] 보안뉴스, “챗GPT 사용해 업무 능력 향상하려다 민감한 정보와 기밀까지 입력해”, Mar. 2023.

[8] 이코노미스트, “[단독] 우려가 현실로…삼성전자, 챗GPT 빗장 풀자마자 ‘오남용’ 속출”, Mar. 2023

[9] 소프트웨어정책연구소, “생성 AI 산업 생태계 현황과 과제”, *SPRI ISSUE REPORT*, IS-165, pp. , Nov. 2023.

[10] 한국인터넷진흥원(KISA), “클라우드 서비스 보안인증 CSAP (isms.kisa.or.kr)”, Apr. 2024.

[11] 행정안전부, “행정기관 및 공공기관의 클라우드컴퓨팅서비스 이용 기준 및 안전성 확보 등에 관한 고시”, 제2023-23호, Apr. 2023

[12] 문지민, 윤혜진. “AI 스타트업 어떻게 진화할까 : ‘저비용 고효율’ sLLM 시대 온다_R&D서 상용화로 중심 이동”, *매경ECONOMY - 2220*, pp. 36-37, 2023.