https://doi.org/10.7840/kics.2025.50.2.217

전력산업에서 대규모 언어 모델(LLM) 활용 방향에 관한 연구

김 은 진◆, 신 용 태°

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

Eunjin Kim◆, Yongtae Shin°

요 약

챗GPT의 등장으로 인해 생성형 인공지능 및 LLM 시장이 급속하게 성장하고 있으며, 시장환경에 따라 기업들은 이 기술을 업무에 적용하기 위한 다양한 시도를 진행하고 있다. 전력산업은 다수 국가에서 공공기관이 산업을 영위하는 독점적 형태로 운용되며, 전력의 특성상 전 산업 및 국민의 생존을 직접적으로 관련되는 기반 산업의 특징을 가진다. 따라서 전력산업은 국가적 영향력이 상당히 크며, 해당 산업에 LLM의 활용 방향성과 전략을 확립함으로써 신기술을 활용한 전력산업의 효율화를 도모하여 국가적 효익을 극대화하고자 한다. 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 기술, 정책 등의 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.

키워드 : 대규모언어모델, 경량형언어모델, 전력산업, 초거대 AI
Key Words : LLM, sLLM, Power Industry, Hyperscale AI

ABSTRACT

With the recent emergence of ChatGPT, the generative AI and LLM (Large Language Models) market is experiencing rapid growth. Consequently, leading enterprises are making various attempts to implement these technologies in their operations. The power industry, often operated as a monopoly by public institutions in many countries, is inherently a critical infrastructure sector directly related to the survival of all industries and the population. Thus, the power sector has significant national influence. By establishing the directions and strategies for using LLMs in this sector, the research aims to enhance the efficiency of the power industry using new technologies, thereby maximizing national benefits. The purpose of this study is to meticulously examine the external constraints on using LLMs in the domestic power industry and to propose strategies for applying these technologies in a way that overcomes or circumvents these constraints. Through literature research related to LLMs, this study will analyze the external environment and derive directions for the use of LLMs in the power industry. It is expected that this will lead to the development of a detailed implementation plan for the specialized use of LLMs in the domestic power industry, contributing to its future development.

◆ First Author : Soongsil University Department of IT Policy Management, sonaflux30@soongsil.ac.kr, 정회원
° Corresponding Author : Soongsil University Department of IT Policy Management, shin@ssu.ac.kr, 정회원
논문번호 : 202409-215-A-RE, Received September 21, 2024; Revised October 24, 2024; Accepted October 27, 2024

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. 연구 배경

2.1 초거대 AI의 언어적 능력, 대규모언어모델

챗GPT는 사람과 대화하는 수준의 서비스를 사람에게 친숙한 '챗봇' 형태로 제공하여 인간과 대화하는 수준의 경험 기회를 제공하면서, 단시간에 폭발적인 관심을 끌고 수억 명의 사용자를 확보하였다. 챗GPT은 가장 범용적으로 활용되는 대규모언어모델(LLM, Large Language Model)이라 할 수 있다. LLM은 대규모 사전학습을 통해 광범위한 언어적 지식을 축적한 언어 모델로 정의한다[1]. LLM은 자연어를 학습하여 인간의 언어와 유사하게 문장을 생성하는 언어모델로 차츰 규모가 커지며 초거대 AI로 진화했다. LLM은 순차 데이터의 문맥 또는 컨텍스트를 학습할 수 있는 신경망인 Transformer 모델을 통해 비약적 성능 발전을 이뤘는데, 최근 방대한 파라미터 크기와 데이터 학습을 통한 성능면에서 '초거대 언어모델'로도 불리고 있다[2]. Transformer 모델은 구글에서 2017년 Transformer AI를 발표하면서 혁신을 주도하였는데, 美 스탠퍼드대는 2021년 Transformer를 Foundation Model로 명명하면서, Foundation Model이 AI 패러다임 견인할 것을 예측했다[3,4].

LLM은 다양한 자연어 처리에서 높은 성능을 발휘하는데, 작문, 외국어 번역, 질의응답, 요약 등 응용 분야에서 활용할 수 있다. Transformer를 활용한 Foundation Model로서 LLM은 사전 학습된 자료를 기반으로 문맥을 이해하고 적절한 답변을 제공하는 언어적 이해와 생성에 관한 다양한 작업을 대학 졸업자 수준(챗GPT 사례)으로 수행할 수 있다. 초거대 AI는 음성, 이미지, 영상 등 언어와 연결가능한 다양한 영역으로 확장 추세에 있으나 산업에서는 LLM 위주로 활용되고 있다. 초거대 AI의 언어적 학습능력을 바탕으로 일선 기업들은 내부데이터를 반영하고 이를 통해 특화서비스를 발굴 및 제공하여 직접적으로 업무에 적용하기 위한 다양한 시도 중이다[4].

2.2 초거대 AI의 산업활용

산업 영역별로 특화한 서비스 구현은 크게 2가지 방식으로 발전하고 있다. 첫 번째는 초거대 AI 플랫폼(Foundation Model, 일반지식)의 LLM에 특화된 전문지식을 추가로 학습(Fine-tuning)시키는 방식, 두 번째는 특화 서비스별로 경량화된 AI 플랫폼의 소형언어모델(sLLM)에 일반지식은 다소 부족하나 전문지식 위주로 구축·활용하는 방식이다. 첫 번째 방식은 전문분야 지식뿐 아니라 일반지식으로 확장성과 초거대 AI 플랫폼이 보유한 기본 성능을 보장한다는 강점이 있고, 두 번째 방식은 전문 영역에서 상대적으로 적은 비용으로 높은 요구 성능 달성할 수 있다는 효율성, 내부 설치형에 따른 보안성 강화의 강점이 있다[5]. 특화 서비스 구현 방법을 요약 정리하면 [표 1]과 같다.

산업 특화 서비스를 구현하는 과정은 초거대 AI 플랫폼을 활용하든 특화된 경량형 AI 플랫폼을 활용하든 유사하다. 구현 과정은 사전 학습 및 강화 학습된 AI 플랫폼에 특화된 전문지식을 파인튜닝하고 시스템으로 적용하는 단계로 볼 수 있다. 이러한 산업 특화 서비스를 구현하는 과정을 챗GPT와 전력산업에의 사례를 들어 개념적으로 표현하면 [그림 1]과 같다.

표 1. 초거대 AI를 활용한 산업 특화 서비스의 구현 방법
Table 1. Implementation Methods of Industry-Specific Services Utilizing Hyper-scale AI

방식	초거대 AI LLM + 전문지식 추가	경량화 AI sLLM + 전문지식 추가
장점	일반지식에 대한 확장성, 기본 성능 보장	전문영역 성능 효율, 보안성 확보
단점	보안 취약	범용성 미흡

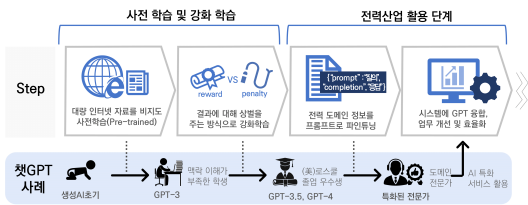

그림 1. 초거대 AI에 산업 특화 서비스 구현 과정
Fig. 1. Implementation process of industry-specific services for hyper-scale AI

Ⅲ. 전력산업의 특징과 고려사항

3.1 전력산업의 특징

국내 전력산업의 밸류체인은 [그림 2]와 같이 발전-송전-배전-영업에 이르는 가치 창출에 직접 기여하는 전통적 본원적 활동과 전략기획-경영관리-ICT 및 R&D 등 가치 창출에 간접 기여하는 지원적 활동으로 구분할 수 있다[6]. 밸류체인의 세부 활동들 향후 LLM을 활용한 전력 특화 서비스로 발굴될 가능성의 영역이다.

발전분야의 약 30%를 차지하는 대기업을 제외하고 국내 전력산업은 공공기관 위주의 반독점적 형태로 운영되고 있다[7]. 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.

그림 2. 국내 전력산업의 밸류체인
Fig. 2. Value chain of the domestic electric power industry

3.2 LLM 보안이슈

3.2.1 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[8]. 때문에 삼성전자, 포스코, 애플 등 국내외 일부 기업은 챗GPT 이용금지 및 제한적 사용 방침으로 하고 있다[9]. 또한, 챗GPT 사칭 앱과 플러그인을 통한 계정 탈취, 악성 프로그램 설치 등 해킹 증가 추세로, 이에 대한 대비책이 시급하다.

3.2.2 배타적 환경을 갖는 기업형 LLM 한계

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

3.2.3 내부설치로 보안이슈를 해소한 sLLM

이러한 보안이슈를 틈새시장 기회로 활용하고자 국내 중소 AI 서비스 업체들은 LLM의 경량화를 통해 비용 효율성을 높인 자체 모델을 개발하거나 및 타사 기반 모델을 보완하여 상업화를 추진하면서 기업 내부에 구축 가능한 온프레미스형 또는 프라이빗 클라우드형 소형언어모델(sLLM)을 판매하고 있다[10]. 이는 전력산업을 넘어 공공 전반에서 보안 이슈 해소를 위한 현실적 대안이 될 수 있다.

3.3 정부 정책 및 제도 한계

3.3.1 망분리 정책

'망분리'란 내부 정보 유출과 인터넷망을 통한 불법적인 접근을 막기 위해 내부망과 기관 인터넷망을 분리하는 네트워크 보안 조치이다. 망분리 정책은 국가정보원의 「국가 정보보안 기본지침」 제 40조를 근거로 하며, 중앙행정부처, 공공기관, 금융기관 및 방위 산업 등은 망분리 정책을 준수해야 한다. 챗GPT 등 초거대 AI 기술을 통한 업무 활용 및 서비스 개발 수요가 크지만, 초거대 AI 플랫폼과 LLM을 이용하려면 외부망 연계가 필수적이라 현행의 망분리 규제와 상충한다. 이에 국정원은 AI 신기술 활용을 주요 내용으로 하는 '사이버시맷코리아 2024'에서 망 보안정책 개선 로드맵을 발표했다. 로드맵의 핵심내용으로는 공공에 획일적으로 적용한 '망분리 정책'을 없애고, 업무를 중요도(기밀 Classified / 민감 Sensitive / 공개 Open)로 구분하고 민감/공개 업무는 적절한 보안 조치를 갖추면 외부인터넷 망과 연결해 업무를 볼 수 있게 하는 '다층보안체계(MLS, Multi Level Security)'를 확대해 나갈 계획이다[11].

3.3.2 전력산업에서 활용 가능한 LLM 부재

앞서 언급한 바와 같이 LLM 서비스 중 정부의 인증을 받은 클라우드 서비스는 없다[12]. 하지만 중앙행정부

처 및 공공기관은 「클라우드컴퓨팅법」(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[13]. 따라서 사실상 전력산업에서는 정부 인증을 받아서 공식적으로 사용가능한 LLM은 부재하다. 주요 기업별 LLM의 보안 및 제도를 비교하면 [표 2]과 같다.

표 2. 주요 기업별 LLM 보안 및 제도 비교
Table 2. Comparison of LLM security and policy by major companies

주요기업 /언어모델	LLM 보안 및 제도 현황 (●적합, ◑ 가능성있음, ○부적합)	
OpenAI /GPT 3.5, GPT 4, GPT 4o	· 보안 별도 배타적 환경 미제공	○ 부적합
	· 제도 미인증, 공공 활용 불가 - 한국을 타겟팅한 인증 계획 없음	○ 부적합
Microsoft Azure /GPT 3.5, GPT 4	· 보안 기업 전용 환경 가능	● 적합
	· 제도 미인증, 공공 활용 불가 - CSAP 인증 취득 준비 중	◑ 인증 시도
Google /Gemini	· 보안 기업 전용 환경 가능	● 적합
	· 제도 미인증, 공공 활용 불가 - 한국을 타겟팅한 인증 계획 없음	○ 부적합
NAVER /하이퍼 클로바X	· 보안 기업 전용 환경 가능	● 적합
	· 제도 미인증, 공공 활용 불가 - CSAP 인증 취득 준비 중	◑ 인증 시도

3.3.3 제약이 없고 기업에 특화된 sLLM

GPT 3.5의 파라미터는 1,750억개, GPT 4는 공개하지 않았으나 약 1조 7,000억개로 추정하며, Gemini는 1조개, 하이퍼클로버X는 2,040억개 등 막대한 파라미터를 가지고 있다. 통상 파라미터가 1,000억개 이상이면 LLM으로, 이하면 sLLM으로 분류한다. 70억개(7B)~500억개(50B)개로 줄인 sLLM이 2023년 하반기 전후로 퍼블릭 클라우드형 뿐만 아니라 온프레미스 및 프라이빗 클라우드형으로도 출시되었다. 국내 주요 중소업체에서 개발한 sLLM을 정리하면 [표 3]와 같다.

sLLM은 보안 이슈에 따른 대안뿐만 아니라 내부 구축이 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 LLM처럼 모든 것에 정통한 AI가 아니라 특화된 도메인 업무를 잘하는 AI가 필요하다는 점에서 sLLM은 LLM보다 적합할 수 있다. 또한 규모가 작으므로 개발·운영비를 상대적으로 크게 절감할 수 있다는 강점이 있다[14].

표 3. 국내 주요 중소업체가 개발한 sLLM
Table 3. sLLM 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	SaaS, 내부구축형
업스테이지	Solar	SaaS, 내부구축형
스캐터랩	PingPong-1	SaaS

3.4 LLM 결과물의 신뢰성

3.4.1 최신성, 정확성 등 한계, 결과 책임 불분명

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. 초거대 AI의 불완전성으로 결과물에 대한 신뢰성을 100% 확신하기 어려우며 결과 책임없는 LLM의 우선 활용보다는, 업무 범위를 한정하여 RAG (검색증강)와 특화된 도메인분야의 sLLM을 활용을 대안으로 검토해볼 수 있다.

3.4.2 비체계적인 신뢰성·성능 평가

초거대 AI 혹은 LLM이 사회와 산업 전반으로 확산되기 위해서는 결과의 신뢰성 확보가 중요하다. 하지만 현재 신뢰성·성능 평가는 일반적인 AI 서비스의 기획·개발 과정에서 개발자 등이 스스로 활용하는 자율점검표, 개발안내서 제공으로 수행되는 수준으로 비체계적으로 수행되고 있다. 향후 정부는 개발된 초거대 AI 혹은 LLM 서비스에 대해 제3의 기관(TTA)을 통한 신뢰성·성능을 평가하고 관련 제도를 수립할 계획이다. 더불어 비윤리·유해성 표현, 사실 왜곡 등을 검증 가능한 데이터 세트를 구축할 계획이다[5].

3.5 해외 공공부문 활용 사례

3.5.1 미국 연방정부 사례

'24년 8월 미국 연방정부 기관인 국제개발처(USAID)가 챗GPT를 활용하여 최초로 업무에 도입한

다고 밝혔다. USAID는 챗GPT 도입으로 행정 업무를 간소화하고 조직들과의 협업을 위한 목적으로 활용할 계획이다[15]. 미국 정부 기관이 OpenAI 서비스 이용 가능한 이유는 애저 거버먼트 클라우드(Azure government cloud)라는 정부 특화 클라우드의 활용 때문이다. 애저 거버먼트 클라우드는 허가된 사용자만 이용 가능하고 독점적 사용을 보장하는 인스턴트를 갖춘 미국 정부 전용 클라우드다. 그러나 OpenAI 서비스는 공공 인터넷과 피어링된 상용 애저 클라우드를 기반으로 한다는데 문제가 있다. 그래서 애저 OpenAI는 FISMA(연방정보보안관리법)에 따라 미국 정부가 준수해야할 보안 기준을 수용하고 이를 증명하기 위해 FedRAMP High 클라우드 서비스 인증을 취득하여 보안 요구를 충족하였다[16].

FedRAMP High 인증은 미국 정부 클라우드 서비스 제공자를 위한 최상위 보안 표준으로 정부의 민감한 데이터를 다루는 데 필요한 보안 요구사항을 충족요건으로 한다[17]. 미국 정부 클라우드에서 OpenAI 서비스 제공을 위해 제공하는 참조 아키텍처는 [그림 3]과 같으며, 주요 보안요건은 [표 4]와 같이 정리하였다.

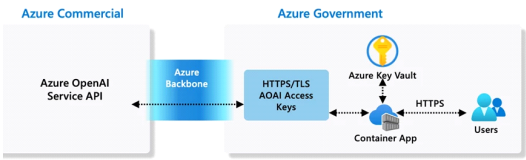

그림 3. 애저 거버먼트의 OpenAI 접근 참조 아키텍처[16]
Fig. 3. Azure Government's OpenAI access reference architecture[16]

표 4. 애저 거버먼트 클라우드에서 OpenAI가 서비스 제공을 위한 주요 보안요건
Table 4. Key Security Requirements for OpenAI Service Provision in Azure Government Cloud

요건	요건 설명
업무 망분리	· 공공 인터넷과 완전 분리(단, 상용 애저 클라우드와 네트워크와 피어링은 인정)
데이터 암호화	· 통신 트래픽 AES-128 이상으로 암호화
데이터 필터링	· 민감데이터 외부 유출 필터링
데이터 저장	· OpenAI에 전송된 데이터는 상용 클라우드에서 작동하지만 저장은 불허
AI학습 미사용	· 정부 데이터가 OpenAI 모델 학습에 사용되지 않음을 보장
지속 모니터링 및 외부감사	· 모니터링과 제3자 보안 검증으로 클라우드 서비스의 보안 위협 조기 탐지·대응

3.5.2 유럽연합(EU) 사례

EU 국가 및 EU 기관들도 행정 업무에서의 효율성 제고를 위해 챗GPT와 같은 생성형 AI의 점진적 도입을 시도하고 있다[18]. EU 집행위원회(European Commission)는 챗GPT를 내부 가이드라인에 따라 사용하고 있으며, 문서 요약, 보고서 작성 등 다소 제한적인 용도로 사용하고 있다[18]. 이는 네트워크 아키텍처 측면에서 내부 업무망에서 직접적으로 OpenAI 서비스를 이용한 사례는 아니다. 제도적 측면에서 볼 때, EU는 FedRAMP High과 같이 진흥을 기반한 보안 인증 제도보다 의무에 기반한 GDPR(일반 데이터 보호 규정)로 개인정보 보호 및 데이터 유출 방지 책임을 부여하고, AI Act로 고위험 AI 분류에서는 사용 제한을 마련하는 등 규제 중심적인 접근을 한다[19].

Ⅳ. 결 론

전력산업에서 초거대 AI 및 LLM을 활용하기 위해 공공부문 도입에 직면하는 보안 이슈, 정책·제도 미흡, 불완전 신뢰성 등 외부환경에 따른 제약적 상황을 알아보았다. 또한 국내 상황과 비견하여 정책·제도 측면에서 참고할만한 해외의 공공부문 사례를 제시하였다. 해당 내용을 통해 전력산업에서 초거대 AI 및 LLM의 활용전략으로 2가지 상반된 접근을 제시하고자 한다.

첫 번째, 외부환경의 구조적 변화와 혁신을 꾀하는 패러다임 시프트 접근이다. 일개 기관이나 개인 풀 수 없는 현재의 보안, 정책·제도적 문제를 거시적 차원에서 돌파하는 방식이다. 국정원의 망분리 완화 및 다층 보안 체계의 도입을 통해서 외부서비스로의 접근을 인가하고, 미국 연방정부 기관의 사례와 같이 안전을 보장하는 클라우드과 FedRAMP High와 같은 인증제도를 활용하면 현재의 보안, 정책·제도적 제약은 상당수 해결될 수 있다. 이를 위해 전력산업 주요 기업은 AI 신기술에 대한 요구를 지속해서 정부에 피력하고 제도 개선 및 기술 검증을 위한 샌드박스 제도, 시스템 시범운영 등에 적극적으로 참여해야 한다.

두 번째, 현재의 제한된 환경에서 시도할 수 있는 최적화된 방안을 모색하는 접근이다. 보안, 정책·제도적 문제의 해결은 장시간 소요되므로 현 상황에서 취할 수 있는 최적의 추진계획을 수립하고 적기에 이행하는 것이 현실적이고 실무적인 전략이다. 현재의 외부 제약적 환경에서는, 여건에 맞는 단계적 확대 방안을 도모하는 것이 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 정부 인증을 받은 LLM에 대해 전력 특화 서비스를 본격 추진한다.

그림 4. 제한된 외부 환경을 고려한 국내 전력산업의 LLM 활용 방향
Fig. 4. Strategies for Utilizing LLM in the Domestic Power Industry Considering the Restricted External Environment.

전력산업에서 LLM 활용 전략을 단계와 단계에 따른 예시 실행과제로 정리하면 [그림 4]과 같다.

전력산업에서 초거대 AI 및 LLM의 활용전략으로 두 가지 상반된 접근을 제시하였는데, 현실적 제약을 돌파하는 패러다임 시프트 접근과 현실적 제약에서 최적화된 방안을 찾는 접근은 전력산업과 같은 공공부분에서 취할 수 있는 거시적 접근과 미시적 접근이라고 할 수 있다. 두 가지 접근은 배타적이지 않으며, 전력산업에서는 두 가지 전략을 동시 추진하고, 제약적 상황이 해소되는 시기에는 내부 구축형 sLLM 뿐만 아니라 챗GPT, 하이퍼클로버X와 같은 LLM을 적절하게 활용하도록 상황에 유연하게 대응해야 한다.

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 과제들이 향후 다양하게 도출하고 즉시-단기-중기 실행계획을 마련할 것이다. 또한 LLM의 시장동향, 기술성숙도 및 정부 정책 등 제반 여건을 주시하고, 적기에 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.

References

[1] T. Brown, et al., "Language models are few-shot learners," *arXiv preprint arXiv:2005.14165*, 2020. (https://doi.org/10.48550/arXiv.2005.14165)

[2] S. An, J. Ryu, W. Cho, J. Noh, and H. Son, "Rise of hyper-scale LLM(Large Language Model) and issues," *Software Policy & Res. Inst. Issue Report,* vol. 158, p. 4, Feb. 2023.

[3] A. Vaswani, et al., "Attention is all you need," *Advances in NIPS*, 2017. (https://doi.org/10.48550/arXiv.1706.03762)

[4] R. Bommasani, et al., "On the opportunities and risks of foundation models," *arXiv preprint arXiv:2108.07258*, 2021. (https://doi.org/10.48550/arXiv.2108.07258)

[5] Ministry of Science and ICT, *Strategies to enhance hyperscale AI competitiveness*(2023), Retrieved Apr. 2023, from https://dl.nanet.go.kr/search/searchInnerDetail.do?controlNo=NONB12023000005078

[6] J. Heo, "Analysis of profitability and business strategies by global utility value chain," *Monthly Electr. J.*, pp. 38-51, Apr. 2020.

[7] Korea Electric Power Corporation, *Power Statistics Monthly Report*(2024), Retrieved Feb. 2024, from https://home.kepco.co.kr/kepco/KO/ntcob/list.do?boardCd=BRD_000097&menuCd=FN05030101

[8] Security News, *Using ChatGPT to enhance work efficiency ends up inputting sensitive and confidential information*(2023), Retrieved Mar. 2023, from http://www.boannews.com/media/view.asp?idx=114975

[9] The Economist, *[Exclusive] Fears become reality... Samsung Electronics faces 'Misuse' issues immediately after unleashing ChatGPT* (2023), Retrieved Mar. 2023, from https://economist.co.kr/article/view/ecn202303300057?s=31

[10] J. Ryu, S. An, M. An, and J. Noh, "The current status and challenges of the generative AI ecosystem," *Software Policy & Res. Inst. Issue Report*, vol. 165, pp. 13, Nov. 2023.

[11] ZDNET Korea, *AI to be freely used on public networks as network separation regulations are relaxed*(2024), Retrieved Sep. 2024, from https://zdnet.co.kr/view/?no=20240911162212

[12] KISA, *Cloud Service Security Certification(CSAP)*

(2024), Retrieved Apr. 2024, from https://isms.kisa.or.kr/main/csap/issue/?certificationMode=list

[13] Ministry of the Interior and Safety, *Notification on the Standards and Safety Assurance for the Use of Cloud Computing Services by Administrative and Public Institution*(2023), Retrieved Apr. 2023, from https://www.law.go.kr/LSW//admRulLsInfoP.do?admRulSeq=2100000246118

[14] J. Moon and H. Yoon, "How will AI startups evolve : The era of 'low-cost high-efficiency' sLLM arrives - shift from R&D to commercialization," *Maeil Business ECONOMY*, no. 2220, pp. 36-37, Aug. 2023.

[15] R. Heilweil, *OpenAI reveals first federal agency customer for ChatGPT Enterprise*(2024), Retrieved Aug. 2024, from https://fedscoop.com/openai-chatgpt-enterprise-usaid/

[16] B. Chappell, *Unlock new insights with Azure OpenAI Service for government*(2023), Retrieved Jun. 2023, from https://azure.microsoft.com/en-us/blog/unlock-new-insights-with-azure-openai-service-for-government/

[17] FedRAMP.gov, *FedRAMP Authorizaion & Federal Agencies*(2023), Retrieved Aug. 2024, from https://www.fedramp.gov/federal-agencies/

[18] General Secretariat of the Council, *ChatGPT in the public sector - Overhyped or overlooked?*, Publications Office of the European Union, 2023. (https://doi.org/10.2860/333725)

[19] N. Helberger and N. Diakopoulos, "ChatGPT and the AI Act," *Internet Policy Rev.*, vol. 12, no. 1, Feb. 2023. (https://doi.org/10.14763/2023.1.1682)

김 은 진 (Eunjin Kim)

2002년 2월 : 서강대학교 컴퓨터공학과 졸업
2019년 2월 : 연세대학교 정보대학원 정보시스템학 석사
2023년 3월~현재 : 숭실대학교 IT정책경영학과 박사과정

<관심분야> 데이터 아키텍처, 빅데이터, AI
[ORCID:0000-0003-0588-7168]

신 용 태 (Yongtae Shin)

1985년 2월 : 한양대학교 산업공학과 졸업
1990년 5월 : University of Iowa 컴퓨터학 석사
1994년 5월 : University of Iowa 컴퓨터학 박사
1995년 3월~현재 : 숭실대학교 컴퓨터학부 교수

<관심분야> 정보보호, IoT, 클라우드 컴퓨팅
[ORCID:0000-0002-1199-1845]