다계층 AI 연합학습을 활용한 자기진화형 BEMS 연계 전력수요 예측 플랫폼 구성에 관한 연구*

장현규[O], 박윤근, 황명하, 주정현, 강희운, 권유진, 이현우, 안수명
한국에너지공과대학교, 한국에너지공과대학교, 전력연구원, 전력연구원, 전력연구원, 전력연구원, 한국에너지공과대학교, 한국에너지공과대학교
hkjang@kentech.ac.kr, yonggamman@kentech.ac.kr, mh.hwang@kepco.co.kr, jh.joo590@kepco.co.kr, heewoon.kang03@kepco.co.kr, kwon43@kepco.co.kr, hwlee@kentech.ac.kr, sumyeongahn@kentech.ac.kr

Design of a Self-Evolving Electricity Demand Forecasting Platform Intergrated with BEMS Based On Multi-Layer Federated Learning

Hyunkyu Jang[O], YOONKEUN PARK, Myeong-Ha Hwang, Jeonghyun Joo, Heewoon Kang, YooJin Kwon, Hyunwoo Lee, Sumyeong Ahn
KENTECH, KENTECH, KEPRI, KEPRI, KEPRI, KEPRI, KENTECH, KENTECH,
hkjang@kentech.ac.kr, yonggamman@kentech.ac.kr, mh.hwang@kepco.co.kr, jh.joo590@kepco.co.kr, heewoon.kang03@kepco.co.kr, kwon43@kepco.co.kr, hwlee@kentech.ac.kr, sumyeongahn@kentech.ac.kr

요 약

신재생에너지 및 분산전원의 확대에 따라 전력망의 변동성이 증대되고 운영이 복잡해졌다. 이에 대한 해결책으로 그리드에 ICT 기술을 접목하여 전력망에 대해 감시하고 이를 토대로 향후 전력량을 예측하면서 운영하는 시스템이 주목받고 있다. 이러한 시스템의 하나인 빌딩 에너지 관리 시스템(Building Energy Management System, BEMS)은 건물 내 에너지 사용에 대해 전력 수요 예측을 바탕으로한 효율적 관리를 목표로 한다. 본 논문에서는 BEMS의 성능을 높이고 개인정보 보호를 위한 자기진화형 다계층 연합학습 전력수요 예측 플랫폼을 제안하며, 이는 다계층 구조에 연합학습을 적용하여 실현하였다.

1. 서론

현대 전력 시스템은 간헐적이고 예측하기 어려운 재생 가능 에너지원의 공급이 증가함에 따라 수요 패턴의 역동적인 변화를 직면하고 있다. 이러한 변동성에 대응하기 위해 높은 정확도와 해상도를 위한 단기 부하 예측(Short Term Load Forecasting, STLF)이 중요해지고 있다 [1]. 정확한 수요 예측은 계통 운영자가 공급과 수요의 균형을 맞추고, 유휴 발전량을 최적화하며, 안정적인 전력 공급을 유지하는 데에 필수적이다.

하지만 STLF는 두가지 난제를 경험하고 있다. 첫째로, 특히 개별 주거용 부하 패턴이 원격 근무 증가 등으로 인해 더욱 동적으로 변하면서, 개별 주거용 부하 예측의 정확도를 보장하기가 어렵다 [2]. 둘째로, 정확한 예측이 가능하려면 많은 데이터가 교환되어야 하는데, 이는 개인정보보호의 이슈를 남긴다.

본 논문에서는 개인정보보호를 보장하면서 정확도를 올리기 위한 다계층 기반의 연합학습 기술을 제안한다.

* 본 연구는 한국전력공사의 2024년 착수 기초연구개발 과제 연구비에 의해 지원되었음(과제번호:R24XO01-3)

2. 배경

STLF는 수 분에서 최대 일주일 앞의 전력 수요 예측하며, 이를 통해 수요-공급 불균형을 방지하고 전력망 운영을 최적화한다. 정확한 STLF를 위해서는 세부적인 부하 데이터가 필요하며, 이러한 세부 데이터는 BEMS의 스마트 미터(Smart Meter)를 비롯한 IoT 디바이스를 통해 구할 수 있다. 그러나 IoT 데이터는 개인정보 유출 문제가 발생할 수 있는데, 예를 들면 개별 주거의 전력 패턴을 통해 특정인이 집에 머무는 시간대 등을 유추할 수 있다. 이러한 개인정보 유출 문제를 해결하기 위한 대안으로 연합학습(Federated Learning, FL)을 활용한 접근이 주목받고 있다. FL은 여러 독립적인 클라이언트(개별 가구 등)가 자신의 훈련 데이터를 공유하지 않고 협력하여 기계 학습 모델을 훈련하는 기술로서 이를 통해 데이터 파편화 및 고립 문제를 해결하고 각 클라이언트가 개별적으로 훈련한 모델보다 더 정확한 예측 모델을 구축할 수 있다 [3].

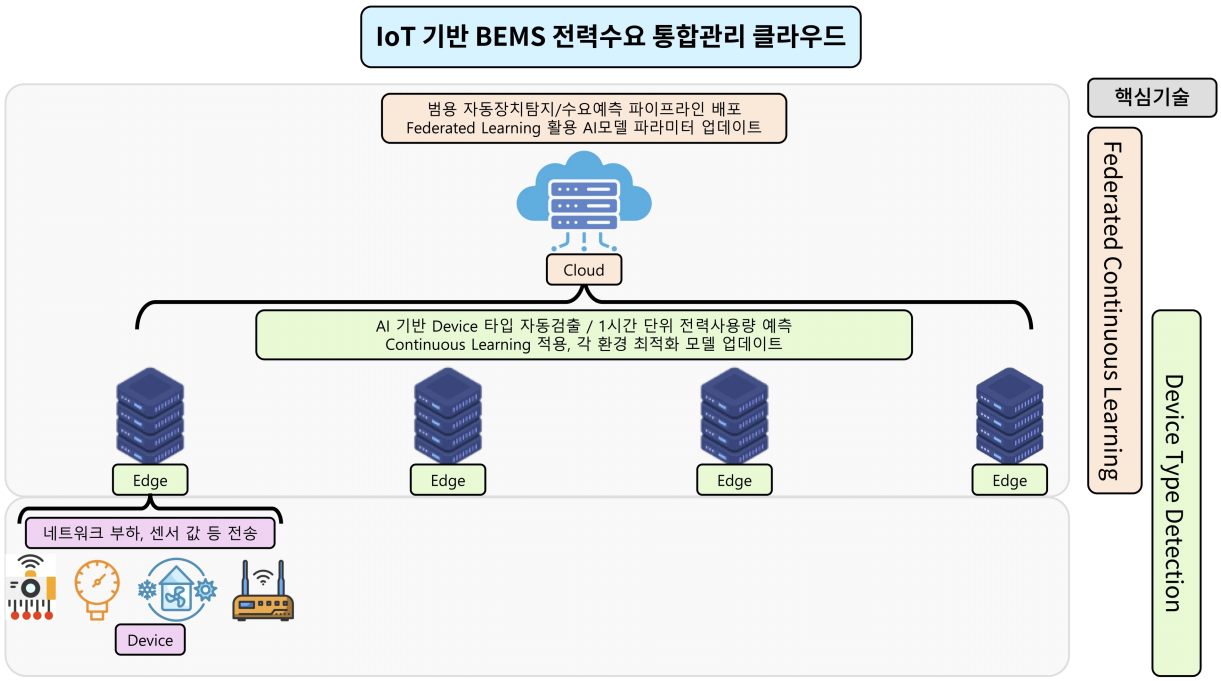

그림 1 프레임워크 디자인 개념도

3. 다계층 AI 연합학습 플랫폼

본 논문은 BEMS에서의 개인정보를 보호하며 동시에 정확도를 높이기 위한 목적으로 다계층AI 연합학습을 활용한 자기진화형 BEMS 연계 전력수요 예측 플랫폼 구성을 제안한다. 플랫폼의 핵심은 클라우드와 엣지(Edge) 단의 협력적인 AI 모델 학습을 위해 연합 학습을 도입하고, 각 환경에 최적화된 모델을 지속적으로 업데이트하는 자기진화 기능을 포함한다.

플랫폼은 기본적으로 아래와 같은 클라우드와 엣지 레벨의 다계층 구조를 갖는다.

- **엣지(가구 단위)**는 개별 건물이나 가정에 설치된 BEMS 및 IoT 장치와 직접 연결되어, BEMS 내 IoT 장치 및 센서로부터 전력 사용량 데이터, 센서 값(예: 온도, 습도) 등 로컬 데이터를 수집하고 전처리하는 역할을 수행한다. 또한 AI 기반으로 기기 유형을 자동으로 검출하고 1시간 단위 전력 사용량 예측과 같은 로컬 예측 및 분석 작업을 수행한다. 연합 학습 프로세스에서는 중앙 서버 역할을 하는 클라우드의 요청에 따라 로컬에서 모델 훈련을 수행하고, 데이터 자체를 전송하는 대신 모델 업데이트(가중치 또는 기울기)만을 클라우드로 전송하는 구조로 데이터 원본의 전송 없이 학습을 수행한다.

- **클라우드(전역 단위)**는 다수의 엣지 노드로부터 수신한 모델 업데이트를 집계하여 전역 모델을 갱신하는 중앙 서버 역할을 수행한다. 또한 연합 학습 전체 과정을 관리하며, 업데이트된 전역 모델을 다시 엣지 노드에 배포하는 역할을 한다. 클라우드는 각 엣지 환경에 최적화된 모델 유지를 위해 지속 학습(Continuous Learning)을 적용하고, 플랫폼 전반의 성능을 모니터링하고 관리하는 기능도 수행한다.

연합 학습은 본 연구가 제안하는 다계층 아키텍처의 핵심 기술이다. 특히 주거용 BEMS 환경의 경우, 여러 가구나 건물이 유사한 라벨의 데이터를 공유하므로 Horizontal FL 구성으로 구현되며, Aggregation 방법으로는 Federated Averaging (Fed-Avg) 방식을 적용하는 것을 제안한다. Fed-Avg는 클라이언트(엣지 노드)가 로컬에서 모델을 훈련한 후 모델 가중치를 중앙 서버(클라우드)로 보내 평균화하여 전역 모델을 업데이트한다.

또한 각 엣지는 Private Model을 적용해 자체 최적화된 가중치를 유지한다. 입력층과 일부 특성 추출층은 로컬 전용으로 분리하고, 전역 모델로 공유되는 파라미터는 상위 계층으로 제한하여 non-IID 특성을 반영하면서도 일반화 성능을 유지할 수 있다 [4]. 클라이언트 전용 파라미터는 서버로 전송되지 않아 역공학 공격 위험을 줄이고, 모델 경량화로 실시간 추론에도 유리하다.

자기진화 기능은 지속 학습을 통해 구현된다. 이는 플랫폼이 새로운 데이터를 지속적으로 수집하고, 이를 바탕으로 엣지 및 클라우드 레벨의 AI 모델을 주기적으로 또는 필요에 따라 업데이트하여 변화하는 부하 패턴이나 환경에 동적으로 적응할 수 있도록 한다. 이를 통해 예측 정확도를 유지 및 향상시키고, 플랫폼의 성능을 시간에 따라 최적화할 수 있다. 한편, 지속학습은 학습 데이터와 테스트 데이터의 분포가 다른 경우에 발생하는 Domain Shift 문

제, 시간의 변화에 따라 데이터의 분포가 달라지는 Concept Drift 문제가 있다 [5][6]. 이를 해결하기 위하여 경험 재생(Experience Replay) 기반 기법 및 도메인 적응(Domain Adaptation) 기법을 적용한다.

4. 발전방향

개인정보보호는 제안하는 플랫폼의 핵심 요소이다. 스마트미터와 BEMS 데이터에는 개인 식별이 가능하거나 생활 패턴을 유추할 수 있는 민감한 정보가 포함되어 있어, 연합 학습만으로는 완전한 프라이버시 보호를 보장하기 어렵다. 특히 연합 학습 중 전송되는 모델 업데이트가 역공학 기법에 악용될 경우, 클라이언트의 민감한 정보가 노출될 수 있다. 실제로 gradient inversion attack이나 model inversion attack과 같은 공격은 모델의 파라미터나 그래디언트를 통해 학습 데이터 원본을 재구성할 수 있음을 보여주었다 [7]. 이러한 위협을 방지하기 위해서는 추가적인 프라이버시 보존 기법의 통합이 필수적이다.

특히, 연합 학습의 핵심 요소인 Aggregation에 암호화를 적용한 Secure Aggregation을 사용할 필요가 있다. 이를 통해 클라이언트와 중앙 서버 간 통신 과정에서 개별 클라이언트의 모델 가중치가 노출되지 않고 안전하게 집계되도록 할 수 있다. SAFELearn은 30만 개 이상의 파라미터를 가진 500개 모델을 0.5초 이내에 집계할 수 있는 효율성을 보이며, 다양한 보안 및 효율성 요구사항에 적응 가능한 유연성을 제공한다 [8]. 이러한 Aggregation은 기존 연합 학습 시스템에 간단하게 적용될 수 있는 만큼, AI의 보안 문제가 중요해지는 현시점에서 유의미한 보안 강화 조치가 될 것으로 기대한다.

5. 결론

본 연구에서는 다계층 AI 연합학습을 이용하여 자기진화형 BEMS 연계 전력수요 예측 플랫폼을 설계하고 그 타당성을 고찰하였다. 제안한 플랫폼은 엣지와 클라우드를 통합한 분산 아키텍처 위에서 연합 학습과 지속 학습 메커니즘을 유기적으로 결합함으로써 주거용 부하 데이터에서의 개인정보를 보호하면서도 예측 정확도를 유지하도록 하였다. BEMS와 연계한 고신뢰 데이터의 확보와 함께 지속 학습 메커니즘을 도입하여 계절 변화와 거주자 행태 변화에 따른 부하 패턴 변동에 실시간으로 적응하도록 하여 장기 운용 시에도 예측 성능을 안정적으로 유지하도록 하였다.
나아가, 보다 안전한 플랫폼 구축을 위해 Sec-Avg 등 연합학습 과정에서 가중치 노출을 최소화하는 Aggregation 방법을 적용하고 데이터 암호화 기법 등을 활용하는 방법을 제안한다.

본 연구가 제안하는 전력수요 예측 플랫폼을 이용하여 벤치마크 데이터셋으로 성능을 검증하고, 실제 BEMS 데이터를 활용하여 실증하는 등 실질적 성능을 확인하고 보안성을 검증하는 후속연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] H. Mansoor, S. Ali, I. U. Khan, N. Arshad, M. A. Khan and S. Faizullah, "Short-Term Load Forecasting Using AMI Data," in *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 22040-22050, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3295617.

[2] P. Ma, S. Cui, M. Chen, S. Zhou, and K. Wang, 'Review of family-level short-term load forecasting and its application in household energy management system', Energies, vol. 16, no. 15, p. 5809, 2023.

[3] Y. Dong, Y. Wang, M. Gama, M. A. Mustafa, G. Deconinck and X. Huang, "Privacy-Preserving Distributed Learning for Residential Short-Term Load Forecasting," in *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 16817-16828, 1 May1, 2024, doi: 10.1109/JIOT.2024.3362587.

[4] Z. Cheng et al., "Privacy-aware joint DNN model deployment and partition optimization for delay-efficient collaborative edge inference," arXiv.org, https://arxiv.org/abs/2502.16091 (accessed May 2, 2025).

[5] M. Zhang, H. Marklund, N. Dhawan, A. Gupta, S. Levine, and C. Finn, "Adaptive risk minimization: Learning to adapt to domain shift," *Advances in Neural Information Processing Systems*, vol. 34, pp. 23664-23678, 2021.

[6] S.-H. An, H.-S. Lee, and S.-H. Kim, "Quantitative Estimation Method for ML Model Performance Change, Due to Concept Drift," *KIPS Transactions on Software and Data Engineering*, vol. 12, no. 6, pp. 259-266, Jun. 2023.

[7] L. Zhu, Z. Liu, and S. Han, "Deep Leakage from Gradients," *Advances in Neural Information Processing Systems* , vol. 32, 2019.

[8] H. Fereidooni et al., "SAFELearn: Secure Aggregation for private FEderated Learning," 2021 IEEE Security and Privacy Workshops (SPW), pp. 56-62, 2021, doi: 10.1109/spw53761.2021.00017.