Privacy-Preserving Transformer-Based Federated Learning AI Models for Power Systems

Summary

The Department of Electrical Power Engineering and Mechatronics at TalTech invites applications for a fully-funded PhD position in the field of AI applications in electric power systems. This project aims to develop privacy-preserving, transformer-based federated learning models tailored for power systems. As smart grids increasingly depend on data-driven intelligence, preserving data privacy across distributed sources like smart meters and substations is a growing challenge. Federated learning allows collaborative model training without centralising sensitive data, but integrating complex architectures such as Transformers while maintaining privacy and efficiency requires further research. This project will explore secure and scalable AI techniques that enhance grid analytics without compromising user confidentiality.

Research field:	Electrical power engineering and mechatronics
Supervisor:	Dr. Tarmo Korõtko
Availability:	This position is available.
Offered by:	School of Engineering Department of Electrical Power Engineering and Mechatronics
Application deadline:	Applications are accepted between June 01, 2025 00:00 and June 30, 2025 23:59 (Europe/Zurich)

Description

This PhD position offers an exciting opportunity to conduct cutting-edge research in AI applications in electric power systems, with a special focus on privacy-preserving applications.

The need for secure, decentralised learning mechanisms grows as digitalisation transforms power systems into data-rich environments. Traditional AI methods rely heavily on centralised data collection, risking user privacy and data breaches. Federated learning presents a decentralized solution, yet including high- performing architectures like Transformers introduces challenges in computational load, training convergence, communication overhead, and privacy risks.

This PhD research focuses on building and evaluating transformer-based AI models within a federated learning framework specific to smart grid applications. Emphasis will be placed on privacy-enhancing technologies (e.g., differential privacy, secure multiparty computation), efficient model aggregation techniques, and real-world data from smart meters and substations.

The goal is to develop scalable, secure, high-performing AI systems that operators can adopt to enhance grid analytics without compromising customer privacy. Results will be validated through simulations and prototype deployments in smart grid testbeds.

Responsibilities and (foreseen) tasks

- Research and development of federated learning frameworks tailored to smart grid data structures.
- Design and implementation of transformer architectures suitable for distributed energy environments.
- Integration of privacy-preserving mechanisms such as differential privacy and secure aggregation.
- Simulation and evaluation of proposed models using synthetic and real-world energy datasets.
- Collaboration with cybersecurity and power system researchers to ensure practical applicability.
- Preparation of scientific publications and participation in conferences.
- Assistance in organizing workshops and dissemination events related to the research topic.

Applicants should fulfil the following requirements:

- Master’s degree in electrical engineering, computer science or applied informatics from the last 5 years
- a clear interest in the topic of the position
- principal understanding of electric power systems and a strong background in AI technology

- Strong programming skills (e.g., Python, TensorFlow, PyTorch)
- excellent command of the English language
- profound writing and analytical skills
- capacity to work both as an independent researcher and as part of an international team
- capacity and willingness to aid in relevant organisational tasks

The following experience is beneficial:

- (co-)authored published scientific papers
- practical experience in working with large datasets, databases and data science
- operations systems engineering

The candidate should submit a research plan for the topic, including the overall research and data collection strategy.The candidate can expand on the listed research questions and tasks, and propose theoretical lenses to be used.

We offer:

- 4-year PhD position in the leading microgrids research group in the region with an extensive portfolio of pan-European and national research and development, and study projects, mainly concerned with renewable energy integration and digital and AI applications in electric power systems.
- The opportunity to conduct high-level research in AI applications in energy systems.
- Access to state-of-the-art research facilities for smart grids and power system digitalisation.
- Opportunities for student exchange through EuroTeQ and Erasmus+ programmes, visits to research conferences and laboratory facilities and networking with leading universities and research centres.

About the department

The Department of Electrical Power Engineering and Mechatronics of Tallinn University of Technology is an interdisciplinary research centre focusing on socially relevant and future-oriented research and teaching issues related to power engineering and mechatronics. The mission of the Department is to be a leader in electrical engineering and technical studies and development projects in Estonia, known and valued in society, and a respected partner in national and international cooperation networks and organizations. The department has coordinated and partnered in several international projects, including Horizon 2020, INTERREG, 7FP, Nordic Energy Research, etc.

The Department of Electrical Power Engineering and Mechatronics conducts research within 7 research groups. It operates state-of-the-art laboratories with high-end equipment, offering accredited services in lighting and different electrical measurements. The department's focus areas are domestic and global challenges related to increasing digitalisation, decarbonisation and decentralisation of electric power systems and increasing use of renewable energy sources. The department carries out research in the following relevant areas:

- Optimisation of electric power systems and system analysis to find possibilities for electrification and decarbonisation
- diagnostics and monitoring of equipment and systems
- cyber-security, 5G data communications and artificial intelligence
- energy networks and research on hydrogen technologies, including energy storage, renewable energy, low carbon technologies, consumption management, and IoT applications in energy
- implementation of smart industry, including industrial robotics, automation, 3D printing, and machine vision
- Implementation of energy and resource efficiency, including digitization of supply chains, mapping of opportunities to optimise systems and reduce energy consumption
- developing smart city solutions, including environmentally friendly and self-driving vehicles/drones, and digital twin applications.

Additional information

For further information, please contact Dr. Tarmo Korõtko tarmo.korotko@taltech.ee

To get more information or to apply online, visit https://taltech.glowbase.com/positions/986 or scan the the code on the left with your smartphone.