Privacy in Energy Systems

Contact points: Aditya (a.pappu@utwente.nl), Bruno (b.endresfrolin@utwente.nl)

Coordination of energy assets is needed for unlocking grid capacity

The rapid adoption of distributed energy resources, electric vehicles, and heat pumps is significantly changing load patterns in distribution grids. This leads to mismatches between intermittent supply and demand, causing congestion and capacity shortages in many countries. Grid operators face rising curtailment and increasing congestion costs, and consumers face growing delays in new connections. However, large-scale infrastructure expansion is slow, expensive, and constrained by workforce limitations, making it insufficient as a standalone solution. These challenges highlight the need for efficient, scalable digital coordination of flexible energy assets, enabling the grid to serve more users with existing infrastructure.

Think of a community with houses that wish to add heavy devices such as EVs and heat pumps but do not get permission to do so since the aggregate energy behaviour could go beyond the limits of the existing grid connection to the community. If the houses can coordinate their energy behaviour such that the aggregate stays well within the allotted limits, this can unlock more space for more devices, but on the same grid connection.

This coordination must be privacy-preserving

Energy management algorithms coordinate the actions of individual assets to ensure their combined behavior achieves a shared objective, such as enhancing grid stability or maximizing community benefits. These objectives may be purely grid-oriented, community-driven, or a combination of both. For example, peak-shaving algorithms guide asset behaviour so that the total power demand is flattened over time. However, such coordination must be designed keeping in mind the design principle that 'each level in the energy grid only has access to the minimum information it needs to achieve its goal'.

The community may adopt peak-shaving as the optimization objective, which requires them to coordinate the energy behaviour. However, the aggregate behaviour of the community goes to grid agents such as an aggregator or a DSO. Such grid agents are interested in the aggregate behaviour of the community and not in the individual behaviour of each house. Therefore, the DSO or aggregator must have access to the aggregate behaviour, but not to individual behaviours that make up this aggregate.

Homomorphic encryption (HE)

Being able to work on secure aggregates such that information about the individual contributions making up the aggregate is not revealed is called the secure aggregation problem. There are many approaches in the literature that try to find solutions to the secure aggregation problem, such as differential privacy, secure multi-party computation, and homomorphic encryption. In this project, we wish to investigate the outcome of using homomorphic encryption with energy management algorithms. Specifically, this project aims to answer the following research questions:

1. Which HE approach is best suited for collaborative optimization in energy systems?
2. How computationally efficient is HE for collaborative optimization in energy systems?

Some references to understand the context

[1] https://www.dutchnews.nl/2025/10/14000-companies-waiting-to-connect-to-dutch-power-grid/

[2] https://freedomlab.com/posts/why-the-decentralization-of-the-energy-system-is-shifting-from-ideal-to-imperative

[3] https://www.youtube.com/watch?v=lNw6d05RW6E

[4] https://student.cs.uwaterloo.ca/~cs492/papers/7foundationalprinciples_longer.pdf