

Privacy-Preserving Clusterized Federated Learning Framework for Energy Forecasting

AMAIA GIL, LUCÍA MUÑOZ,
ANTONIO NAPPA, IZAR AZPIROZ

Departments: **Digital Security, Data Intelligence for
Industry, Energy and Environment**



lmunoz@vicomtech.org

vicomtech

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

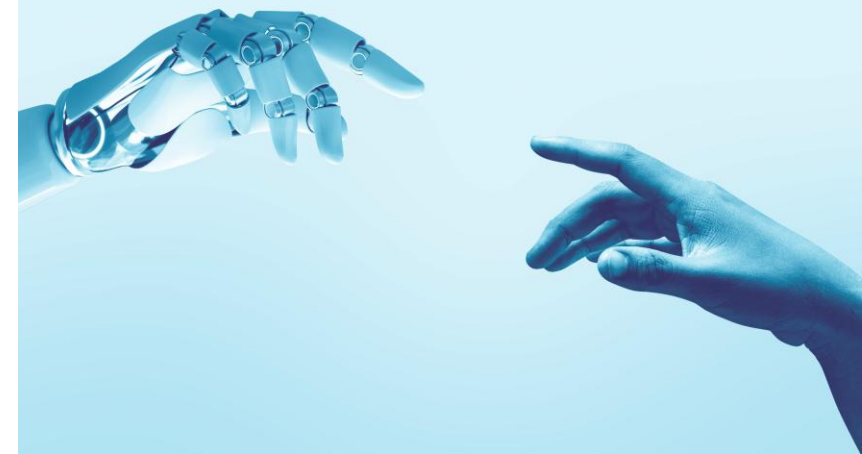
INDEX

01 INTRODUCTION &
CHALLENGES

02 METHODOLOGY

03 RESULTS

04 CONCLUSIONS

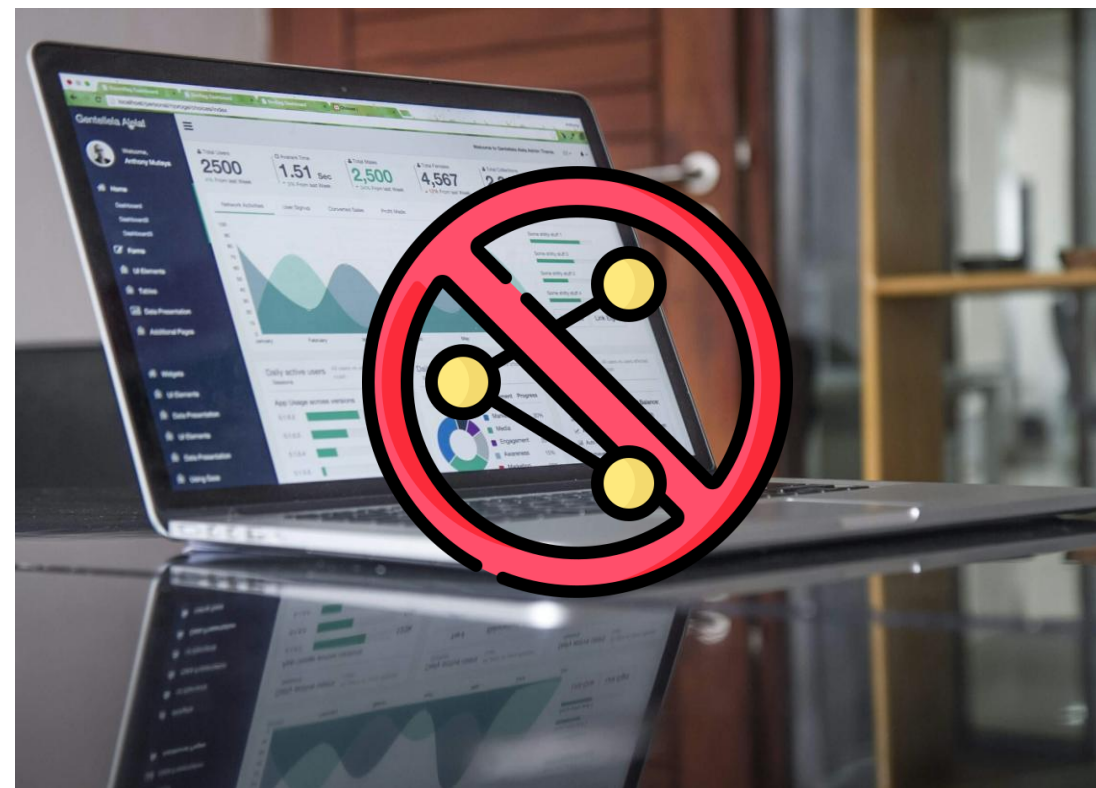


INTRODUCTION & CONTEXT

Adoption of Artificial Intelligence in **competitive industrial sectors** is slowed down by:

- Limited data.
- Restrictions on sharing it.

This is critical in the **energy sector**, where consumption patterns can reveal users' private behaviors



CHALLENGES



Federated Learning

... BUT ...

- Model parameters are still sensitive
- Demand profiles are heterogenous

PROPOSED SOLUTION

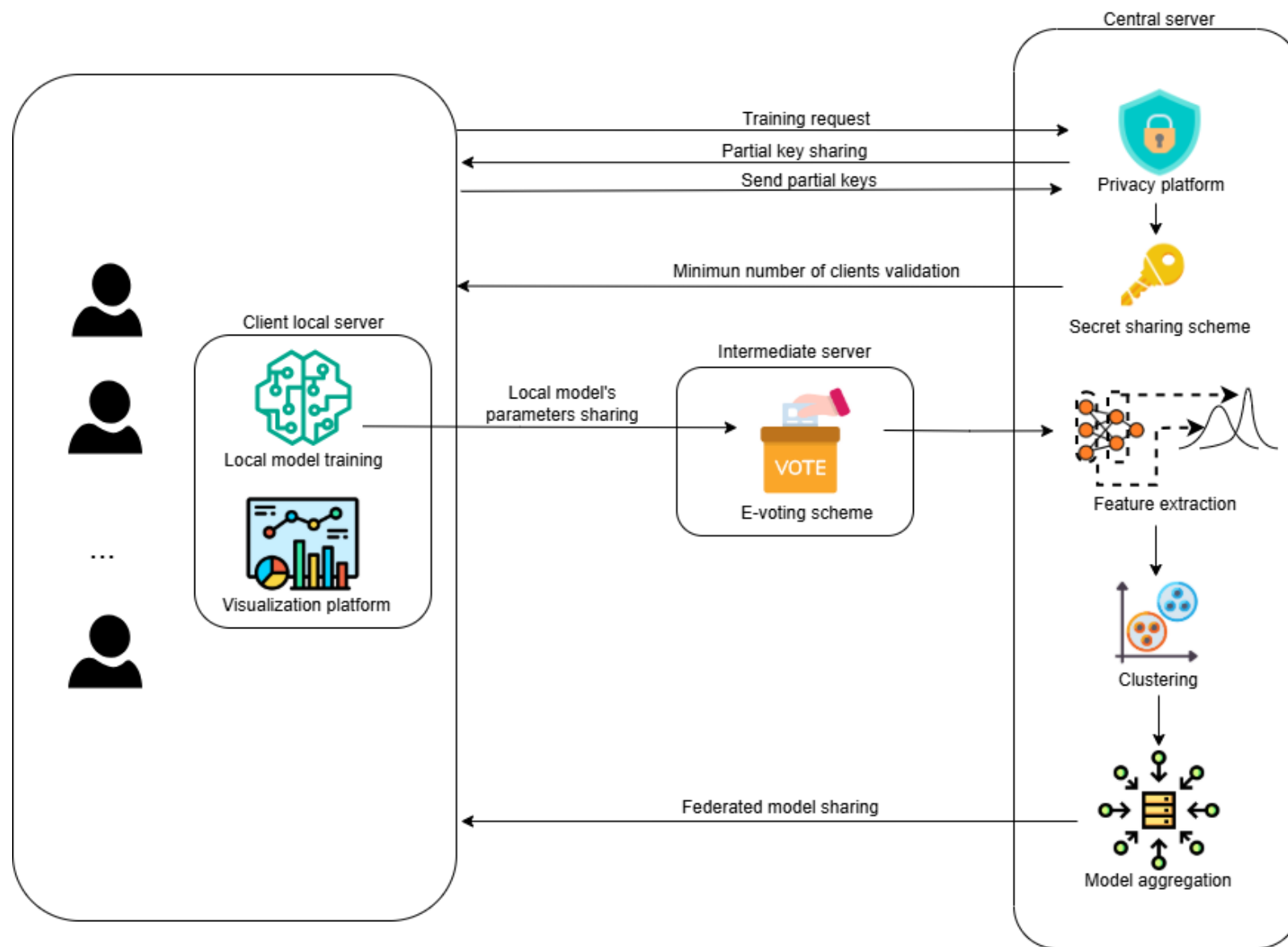


... BUT ...

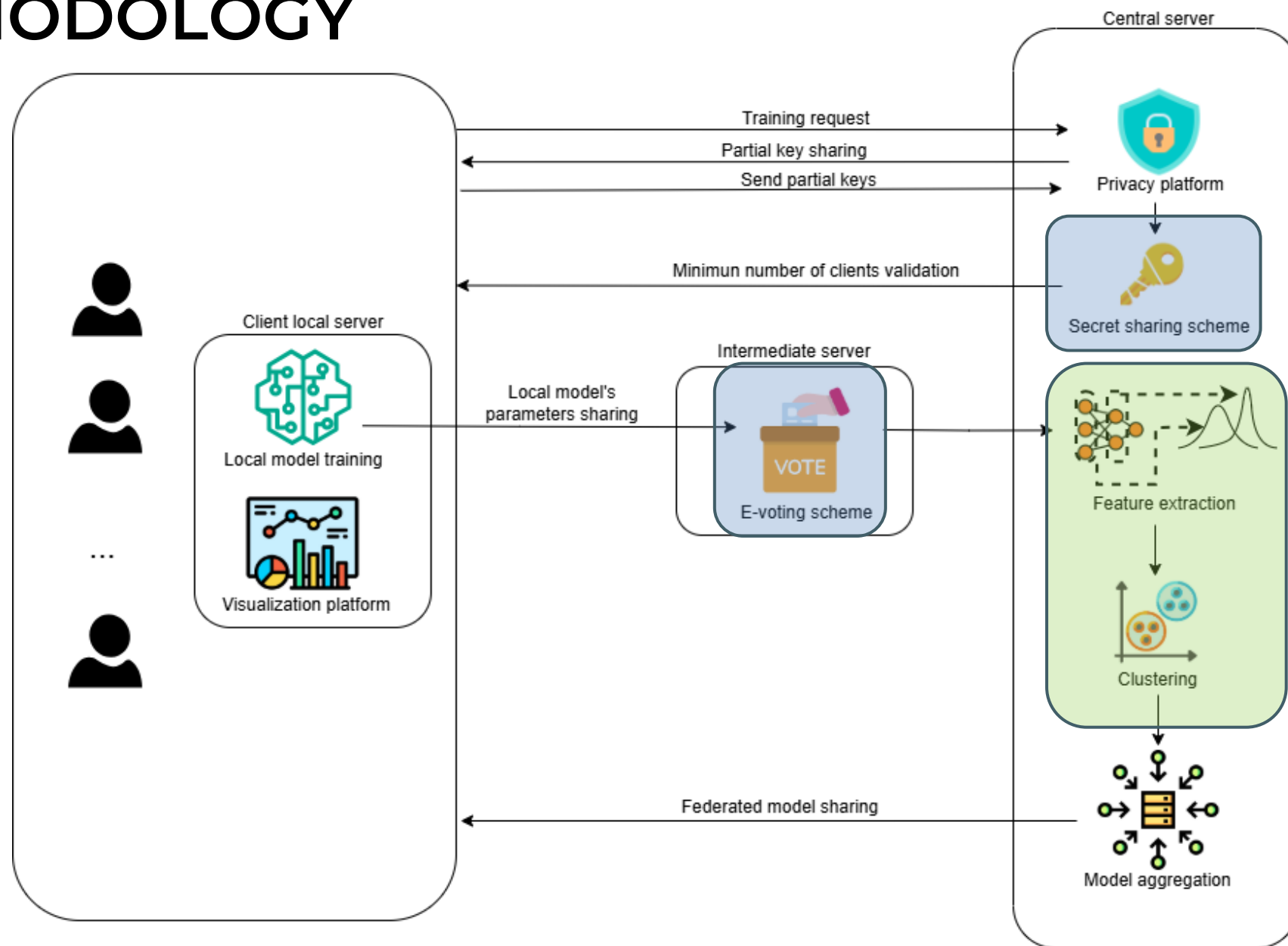
- Model parameters are still sensitive
- Demand profiles are heterogenous



METHODOLOGY



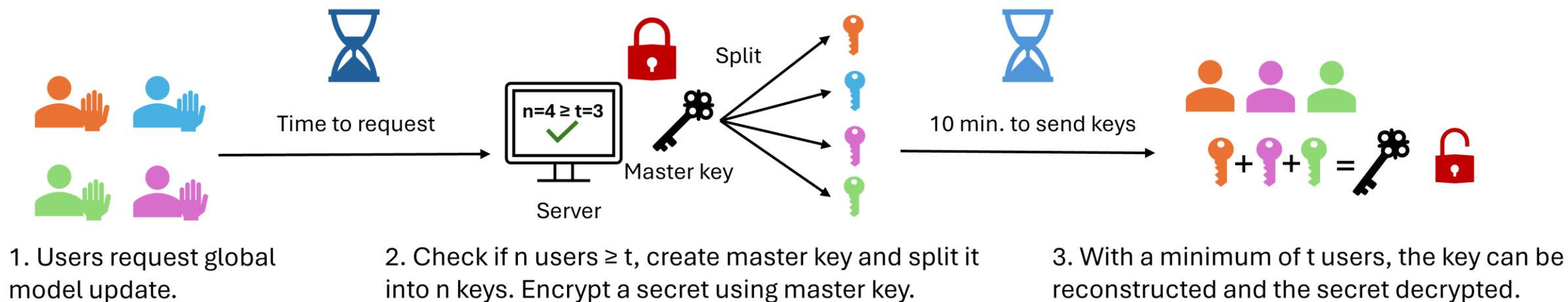
METHODOLOGY



PRIVACY STRATEGIES

TRAINING REQUEST

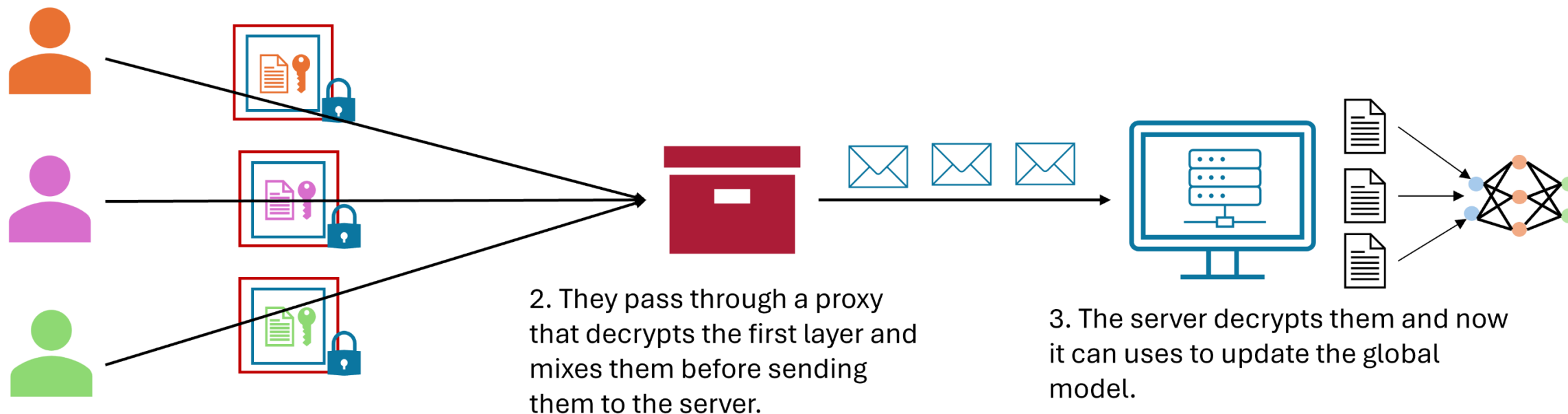
- SECRET SHARING SCHEMES: Shamir's algorithm
- Ensure Minimum Number of Clients in a temporal window



PRIVACY STRATEGIES

MODELS' PARAMETERS SHARING WITH CENTRAL SERVER

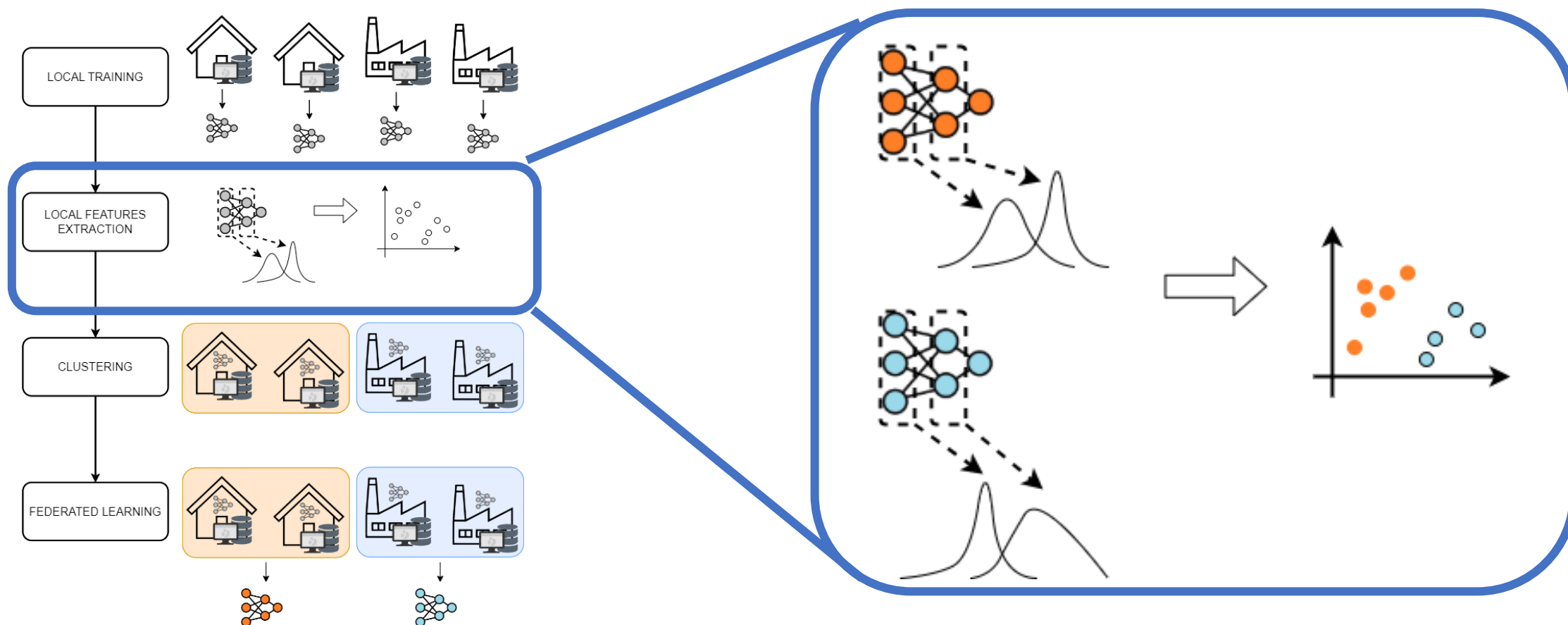
- E-voting inspired algorithm with encrypted data (ElGamal+AES algorithm)
- Anonymous Local Model's parameters Sharing



1. Users send encrypted model parameters to the server.

CLUSTERING

- Parameter values density distribution for feature extraction
- DBSCAN algorithm for clustering



RESULTS – PRIVACY STRATEGIES

- Functional prototype with **dashboard** for local training and encrypted parameter sharing.
- **Temporal validation window** for key exchange and anonymized aggregation.
- Protocol executed efficiently, with minimal overhead — validated rounds only when threshold ≥ 3 clients.


ASTER: Building 61



 LOGOUT

Local AI Model

Download **AI Model** to run the model locally with your own data.
This program generates a `.zip` file with your parameters. Use it to update the federated model.


[DOWNLOAD AI MODEL](#)



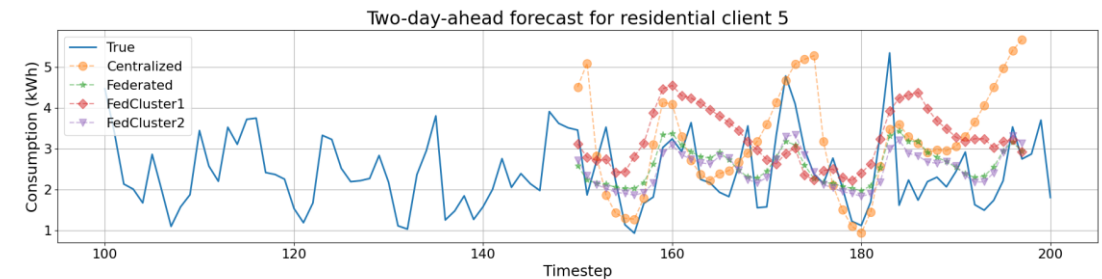
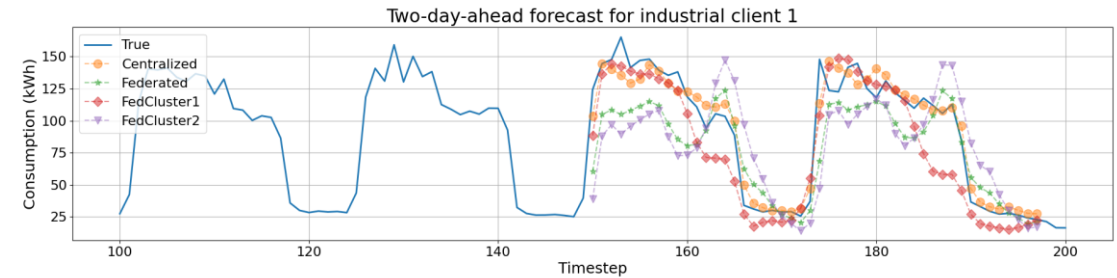
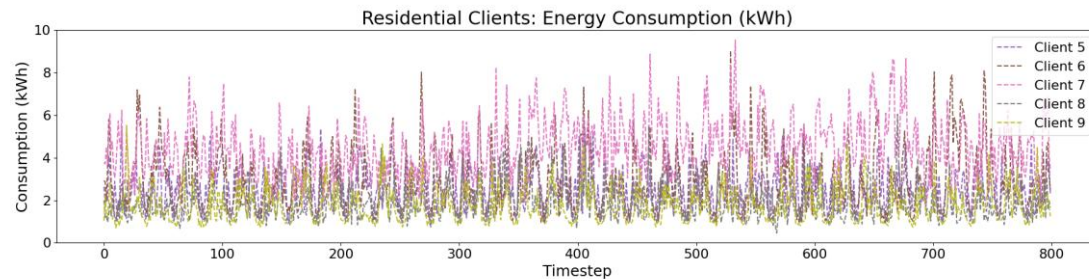
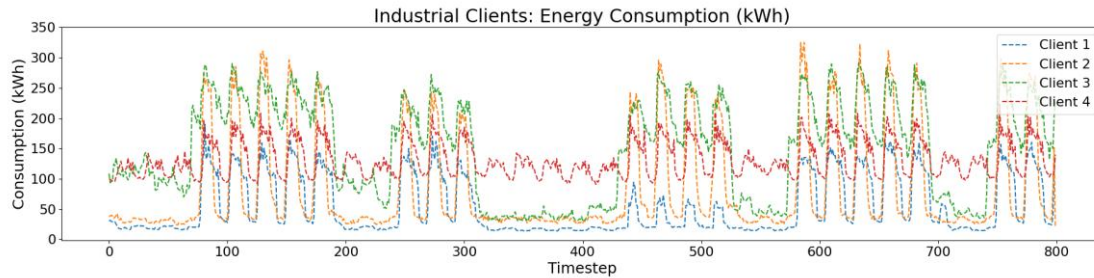
Federated Training

Federated model actualization is available from **12am to 14pm**.

You can request participation.

[REQUEST TRAINING](#)

RESULTS – FEDERATED MODEL



- The clusterization step **detects two subgroups**, which correspond to industrial and residential clients.
- The clusterized federated model belonging to **industrial users** reaches **competitive forecasting** results when compared to the "idealized upper bound" of the centralized scenario.
- When considering the highly irregular patterns of **residential energy consumption**, the clusterized federated model belonging to residential users **outperforms** every other model (the federated models and the centralized one).

CONCLUSIONS

PRIVACY

- Secure and anonymous client participation
- Negligible communication overhead

PERFORMANCE

- Clustered FL improves accuracy under heterogeneity
- Industrial $\approx$ centralized results
- Residential $>$ centralized



Next steps: adaptive clustering, async updates, large-scale validation

ANY QUESTIONS?
THANK YOU!



Imunoz@vicomtech.org



www.vicomtech.org