The University of Manchester

KU LEUVEN

The AAAI's Workshop on
Artificial Intelligence Safety

SafeAI

Privacy Friendly Energy Consumption Prediction: Real Use-Case Scenario

Mustafa A. Mustafa, James Nightingale (UoM)
Yingjie (Tony) Wang, Fairouz Zobiri, Mariana B. da Gama (KUL)

February 28, 2022

snippet

EnnCore

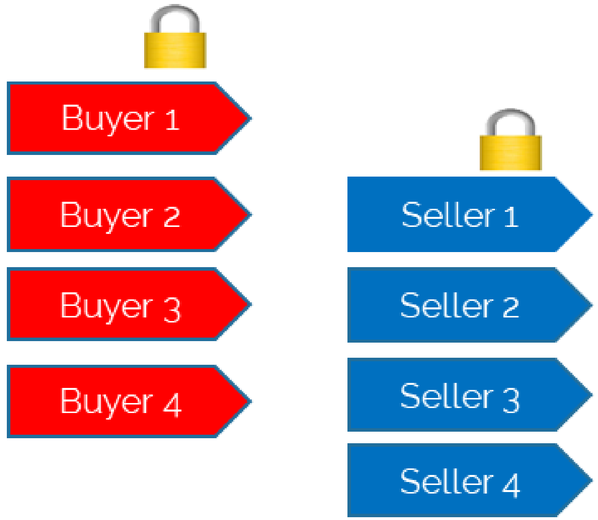
Energy use-case

UrbanChain

UoM start-up who runs a unique energy market place just for renewables

Peer-to-peer energy exchange system that allows

- households (Buyers) to place an order for electricity
- generators (Sellers) to meet that order



The order submission and matching happen in advance of electricity deliver. Hence,

- households (Buyers) need to predict their el. consumption
- generators (Sellers) need to predict their available supply

snippet

EnnCore

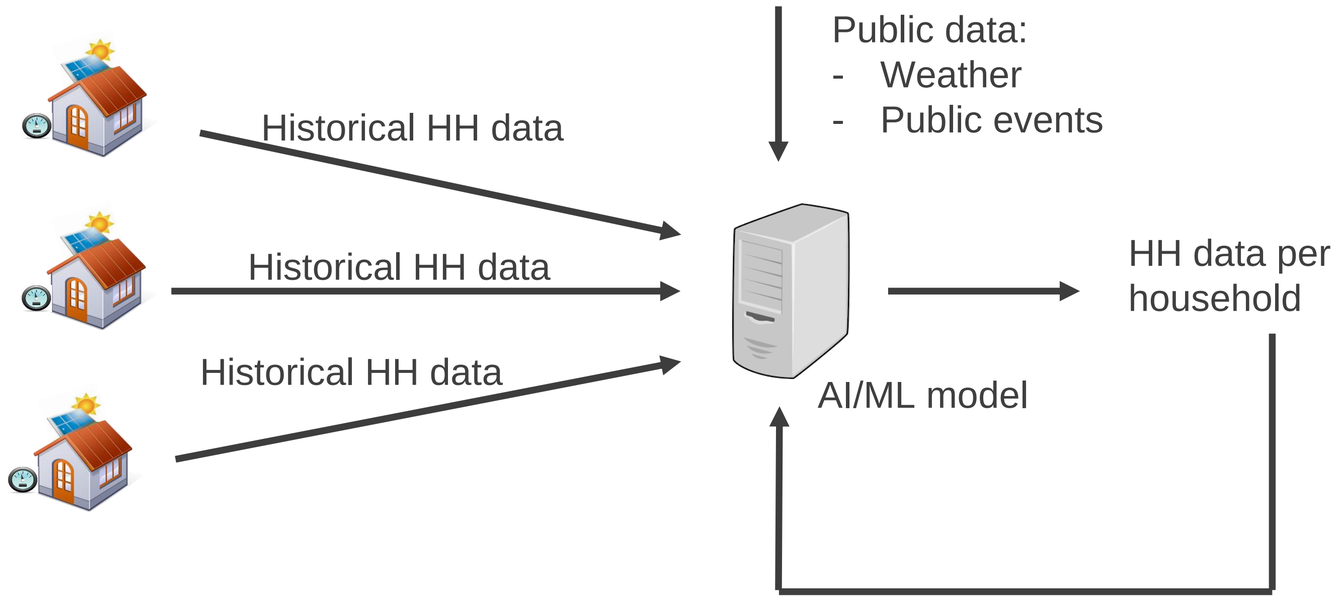
Electricity consumption prediction

Aim of the AI/ML model

- predict the half-hourly (HH) electricity consumption of a household

Private input data:

- Previous HH data: most crucial data
- Number of occupants
- Type of house

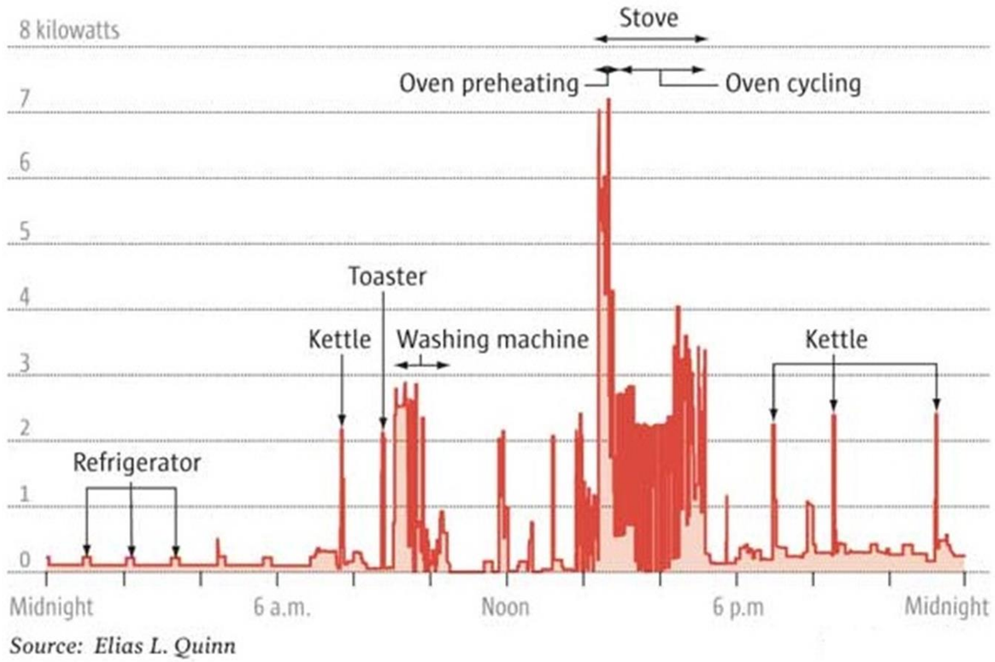


Publicly available data

- Weather forecast/conditions
- Major events (football games, TV programs, lockdown)
- …

Privacy concerns

Example daily load profile of a household



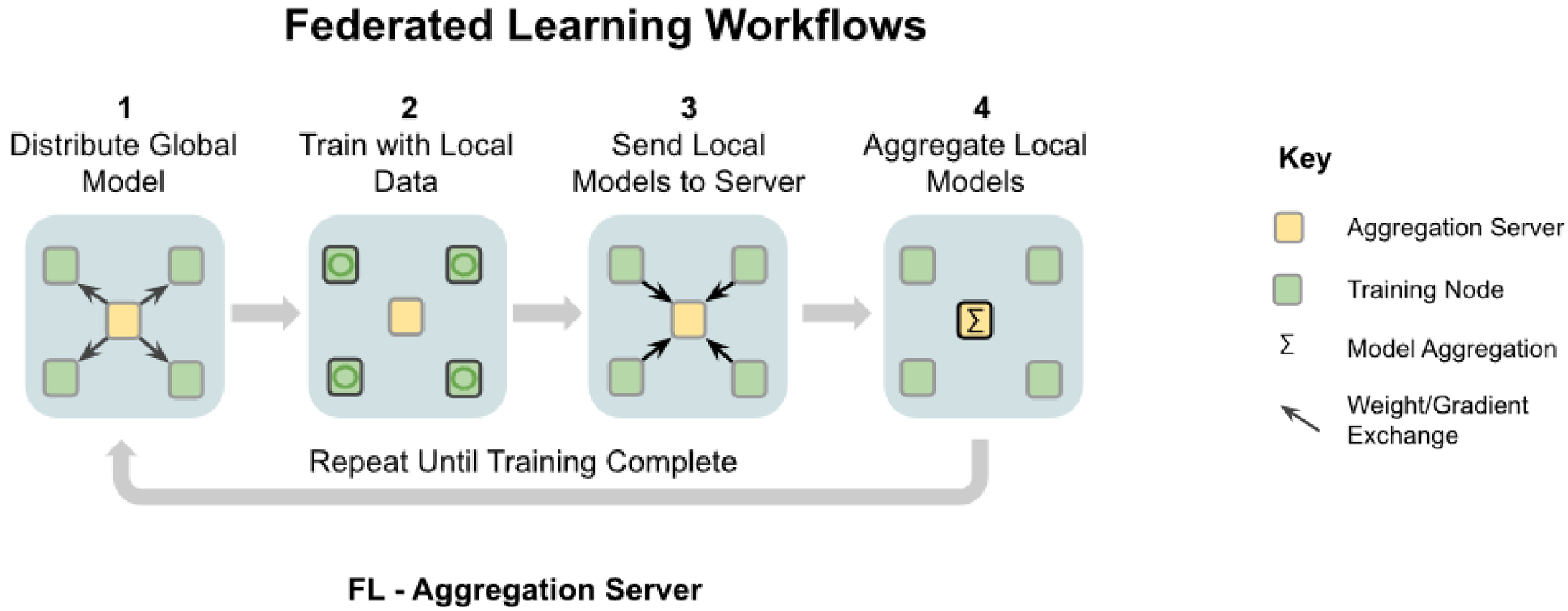
Source: Elias L. Quinn

From load (electricity consumption) profile of a household, one can deduct information such as:

- Number of people
- Habits
- Activities
- Medical conditions
- Religion

Our aim: **design an AI/ML model that is privacy-friendly**

Federated learning



Use-case evaluation

We use real HH data

Smart Metering Electricity Customer Behaviour Trials that took place during 2009 and 2010 with over **5,000 Irish homes and businesses** participating.
https://www.ucd.ie/issda/data/commissionforenergyregulationcer/

Data format

- Meter ID
- Type of premises = residential, SME
- Five digit code: Day & Time codes
- Electricity consumed during 30 minute interval (in kWh)

We developed and tested four ML models:

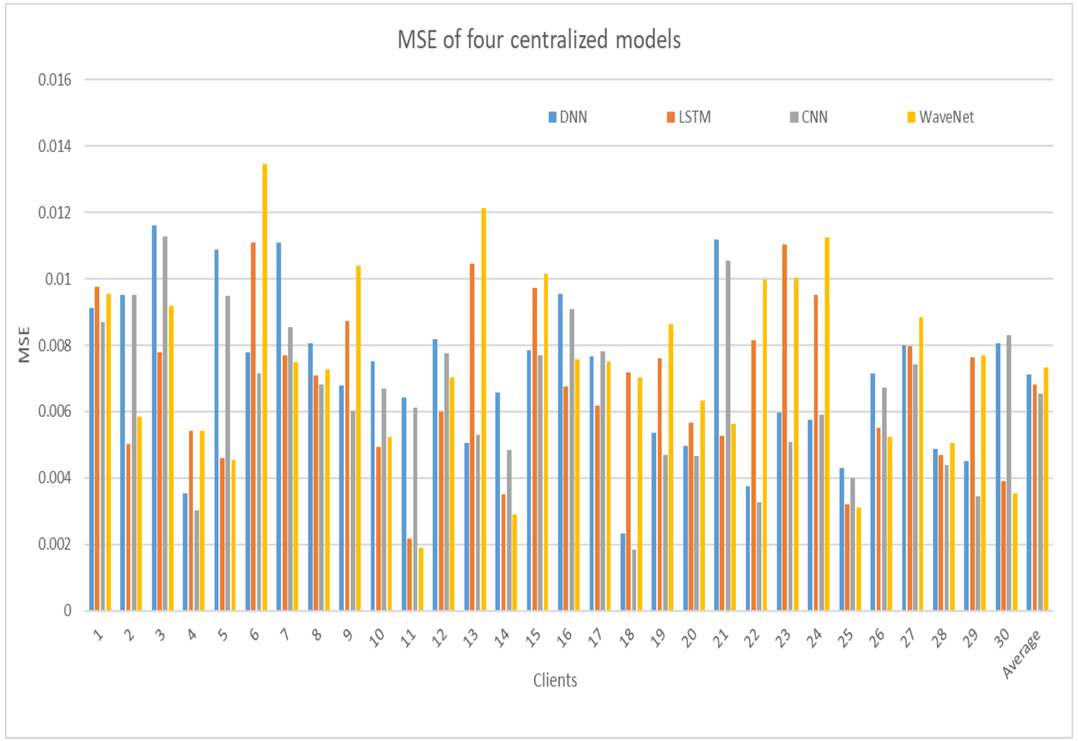
- Deep Neural Network (DNN)
- Long Short-Term Memory (LSTM)
- Convolutional Neural Network (CNN)
- WaveNet

We implemented and compared the four ML models in a centralised and FL framework using TensorFlow.

We evaluated them in terms of:

- Accuracy
- Scalability
- Robustness

Evaluation: accuracy



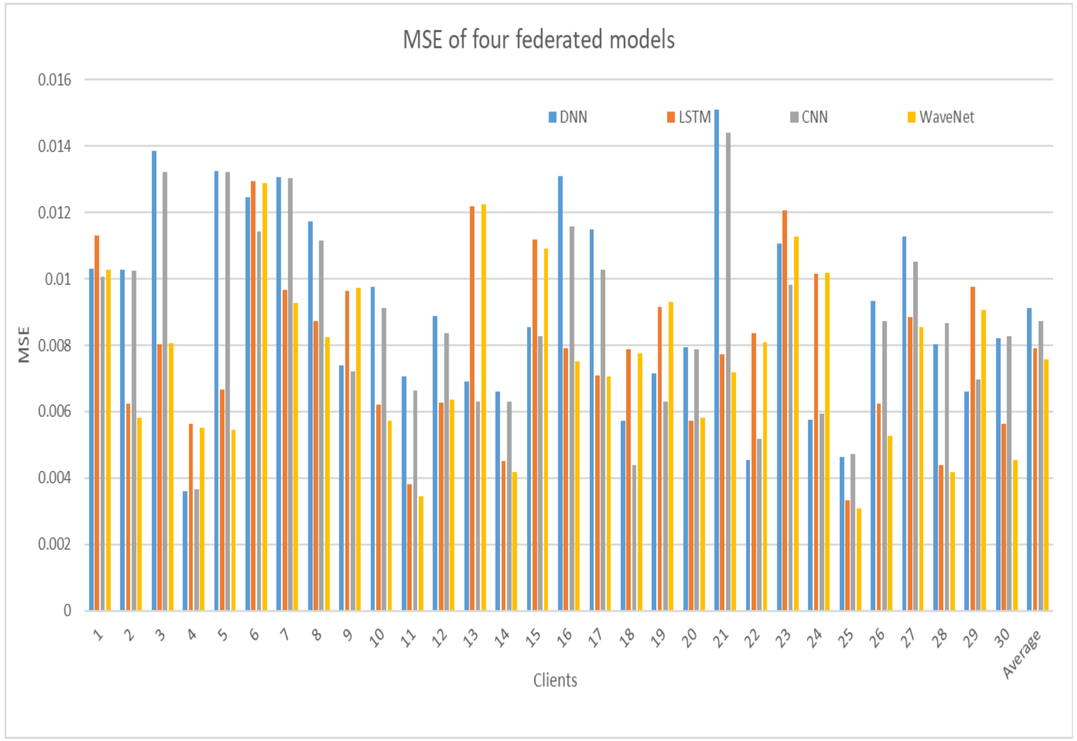


Table I Average MSE and training time

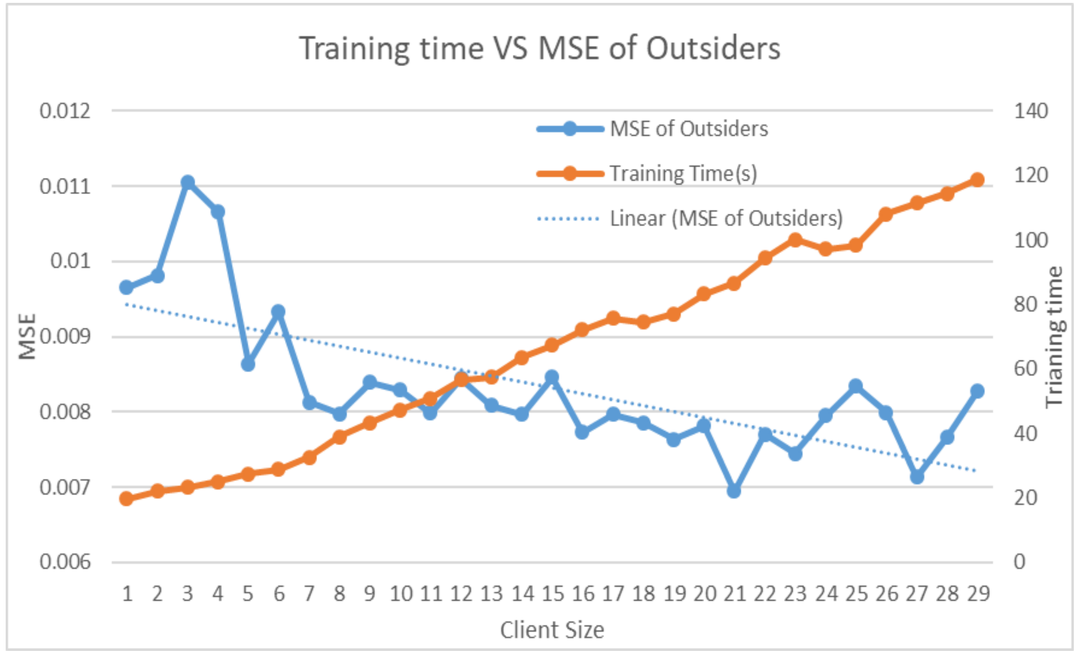
Model	Average MSE		Training time (s)	
	centralized	federated	centralized	federated
DNN	0.007112	0.009125	338.057	121.403
CNN	0.006541	0.008727	4361.669	978.411
LSTM	0.006807	0.007909	18622.955	2476.113
WaveNet	0.007250	0.007566	14458.687	2474.339

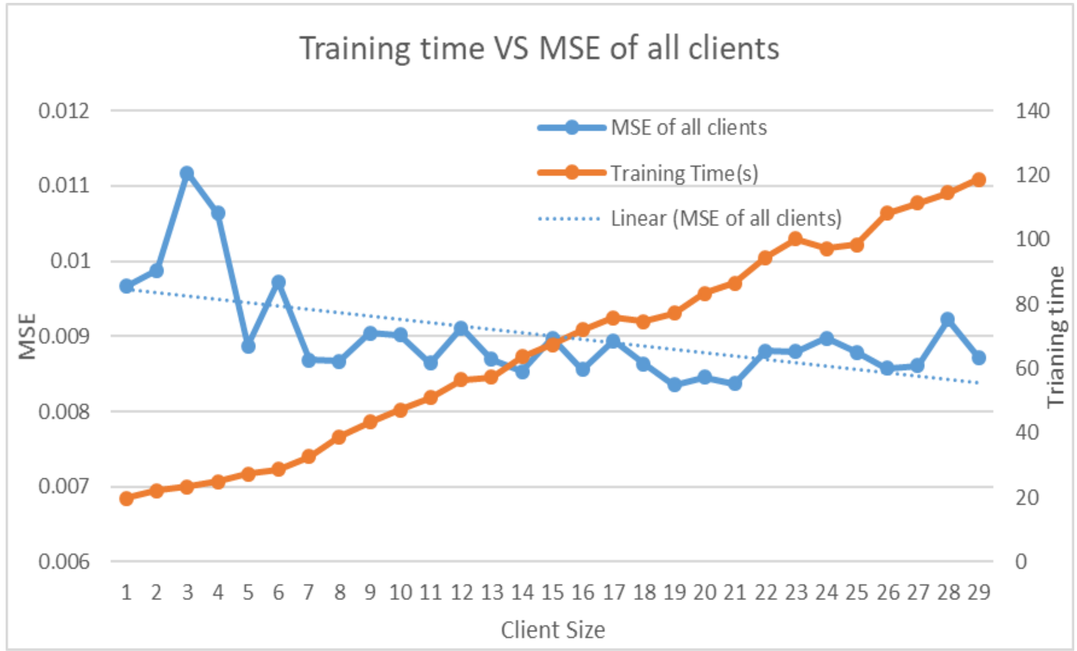
snippet

EnnCore

Evaluation: scalability

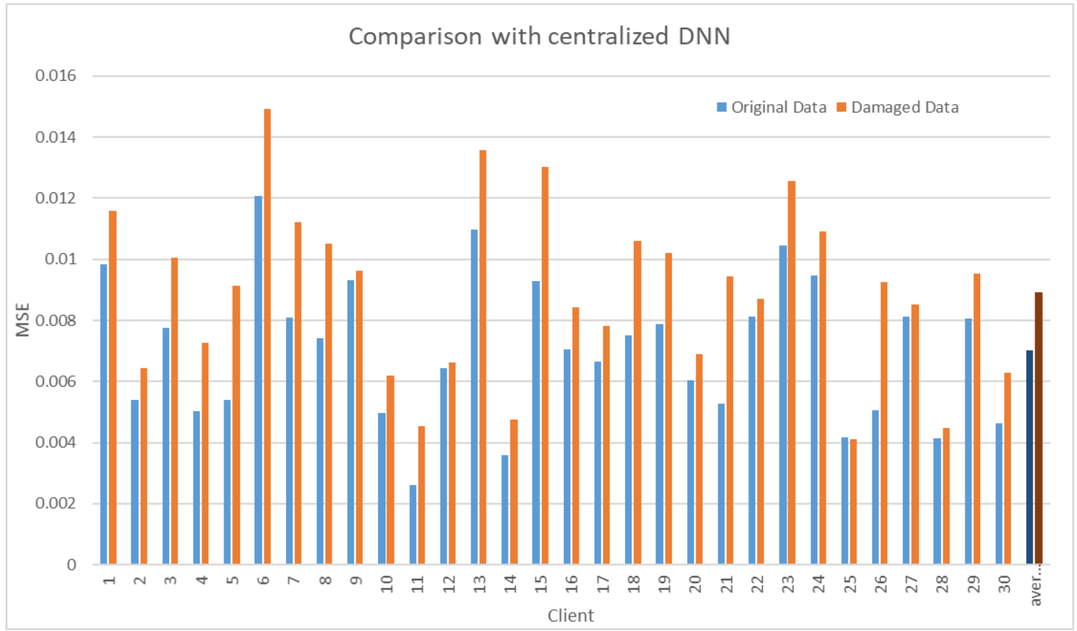
- Form an energy community with member households training collaboratively the ML models
- A community with 8-10 households already generate ML models with good-enough accuracy
- Outsiders of the community could also benefit from the ML models trained by the community

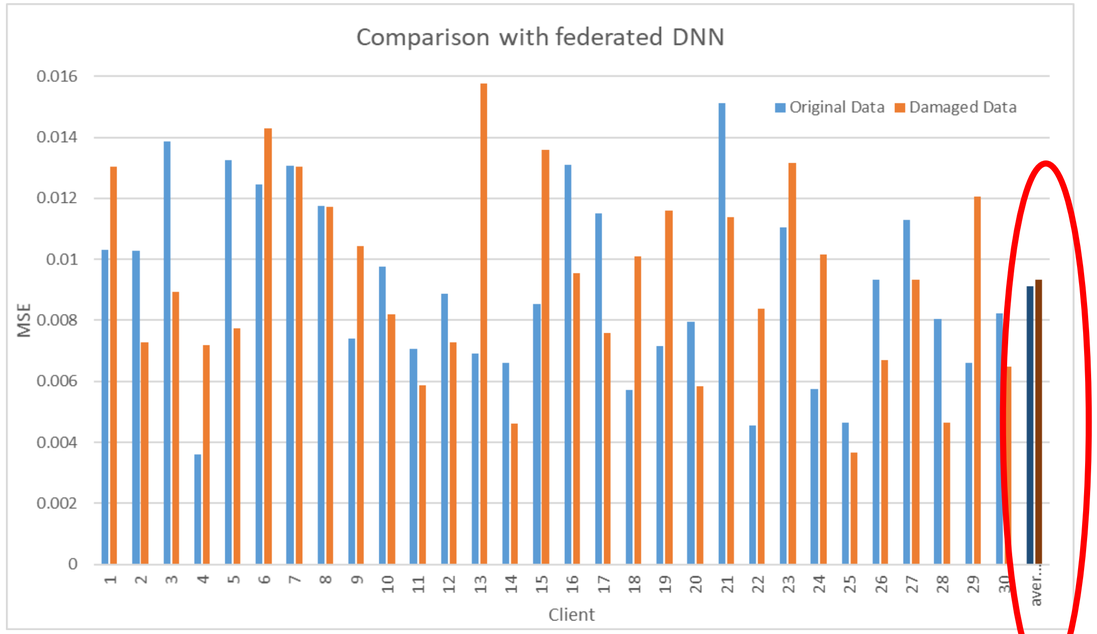




Evaluation: robustness

- 25% of the data used in the training phase is lost (set to zero)
- For each client, the lost data entry is selected randomly





Privacy analysis

- With federated learning, no client raw data leave the client-side **Good!**
- Only individual client gradients' are shared with the central server **Good!**
- Gradients themselves can leak information about the raw data **Not so good!**
- There is too much trust placed on the central server **Not so good!**

We need to protect the gradients too

Conclusions

Take away from our experiments

- Compared to Centralised ML, FL achieves comparable accuracy with improved scalability and robustness
- Pure FL is not sufficient to protect clients' sensitive data

Next steps

- Deploy secure computation techniques (HE and MPC) to protect clients' gradients
- Perform analyses on a larger group of clients (1k+)
- Deploy clustering algorithms on gradients to improve accuracy
- Explore the trade-offs between privacy protection and explainability & verifiability

We are hiring!

Research Associate (Postdoc) in Secure & Privacy-Preserving AI Models

- Application deadline: **8 March 2022**
- More info: https://www.jobs.manchester.ac.uk/displayjob.aspx?jobid=21631
- Contact: mustafa.mustafa@manchester.ac.uk

snippet

EnnCore