# Détection d'intrusions fédérée et semi-supervisée pour l'IoT

PFIA 2022

Ons Aouedi, Kandaraj Piamrat

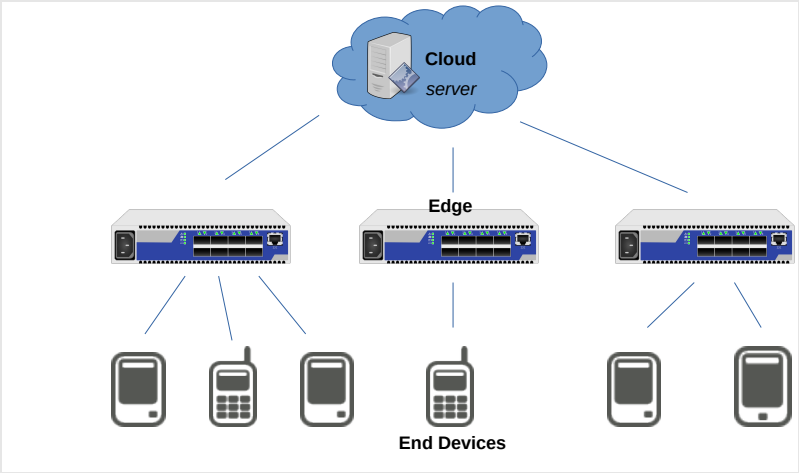
LABORATOIRE DES SCIENCES DU NUMÉRIQUE DE NANTES

**Guillaume Muller**, Kamal Singh

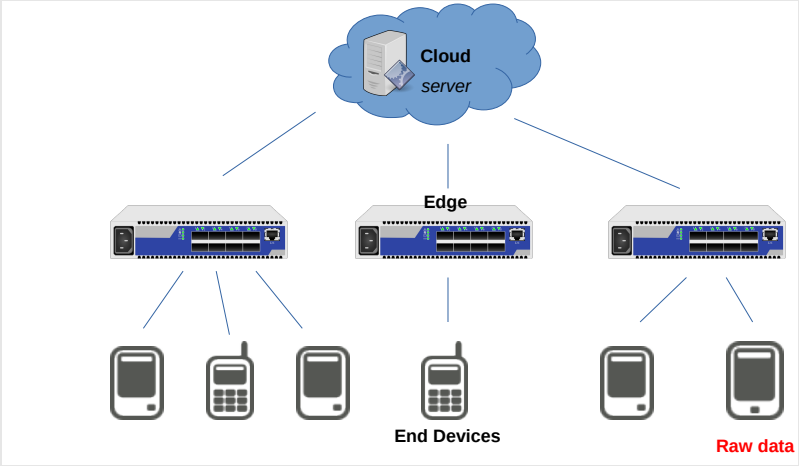
LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

27/06/2022

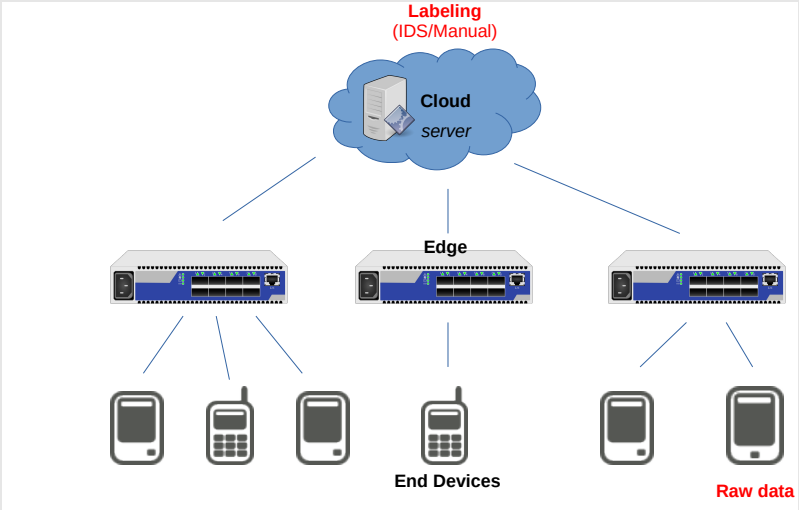
## Contexte



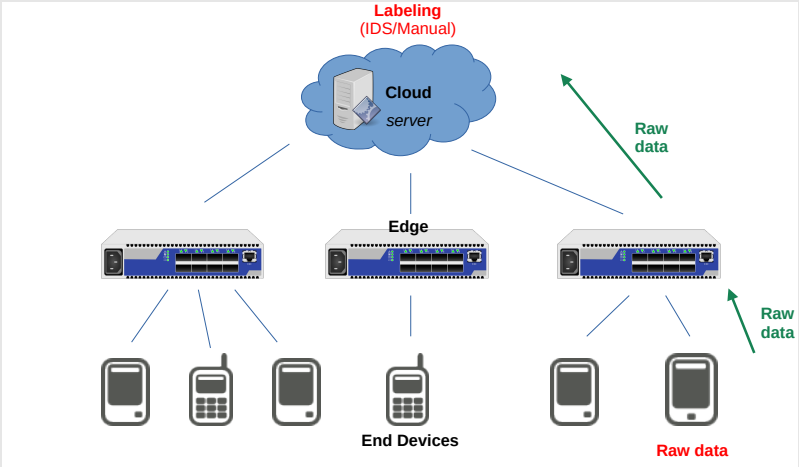
## Contexte



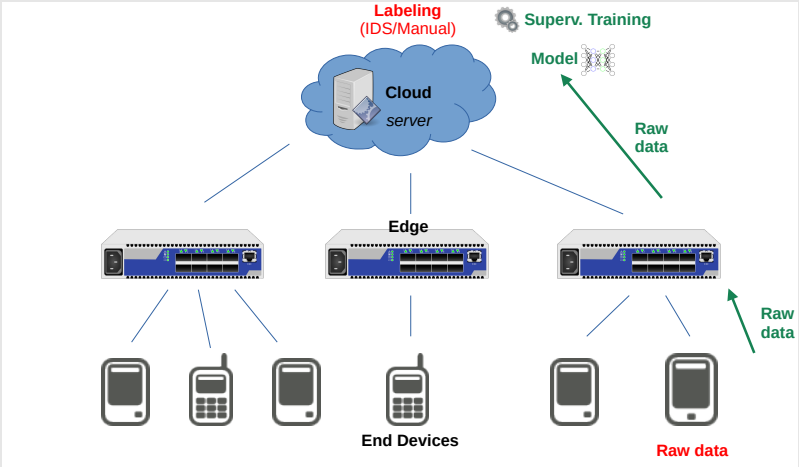
## Contexte



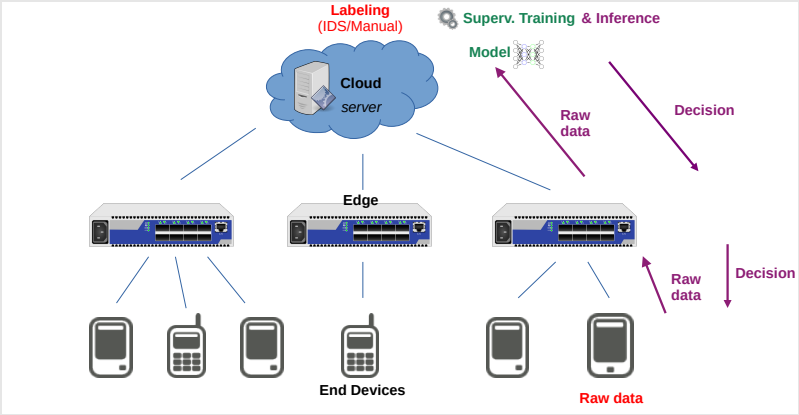
## Machine Learning Traditionnel



## Machine Learning Traditionnel



## Machine Learning Traditionnel



## Synthèse

- **Contexte**
  - Données distribuées sur End-Devices
  - Labels centralisés sur Serveur
  - *Étiquetage coûteux* (👤🕒 + 💵)
- **Machine Learning** utile car adapatif, **mais**
  - Charge réseau (training)
  - Charge serveur (training)
  - Latence (inférence)
  - *Vie privée*

Notre proposition = combiner:

**Federated Learning**

- Distribution
- Vie privée

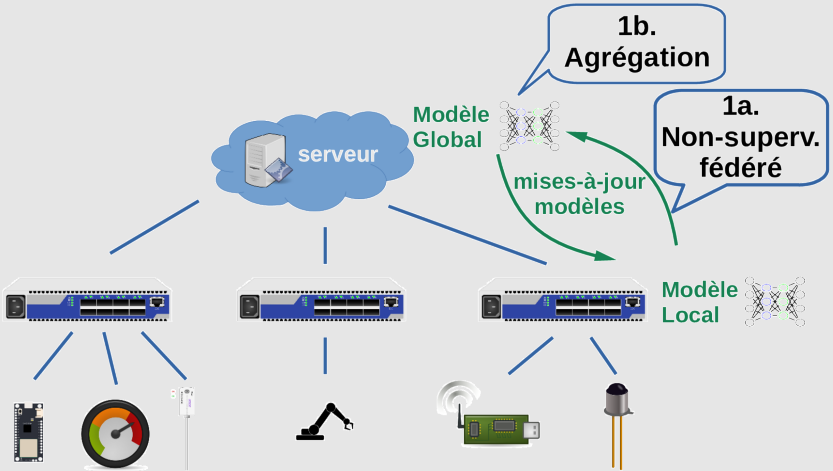
**Semi-supervisé**

- Exploiter les données **Non**-étiquetées

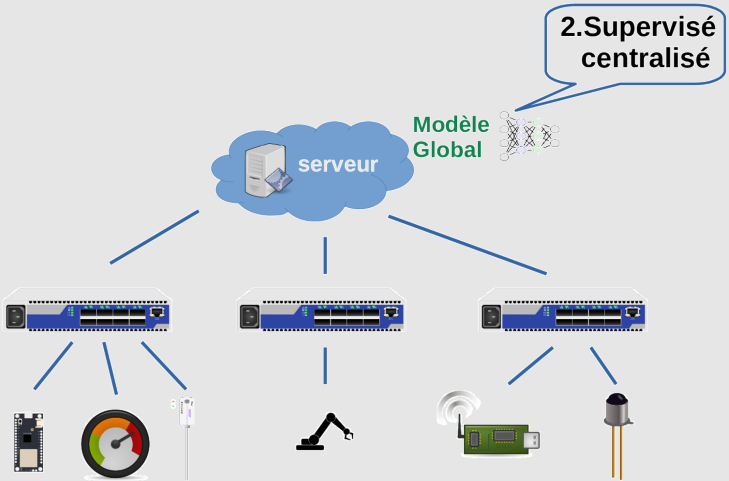
**Lien**

- Auto-Encodeurs
- Split-Learning

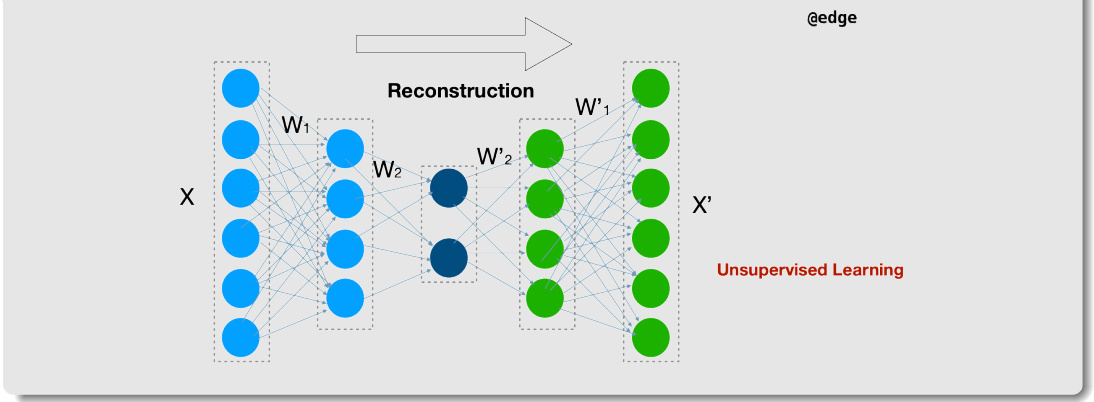
FLuIDS


1b.
Agrégation
1a.
Non-superv.
fédéré
Modèle
Global
serveur
mises-à-jour
modèles
Modèle
Local

## FLuIDS

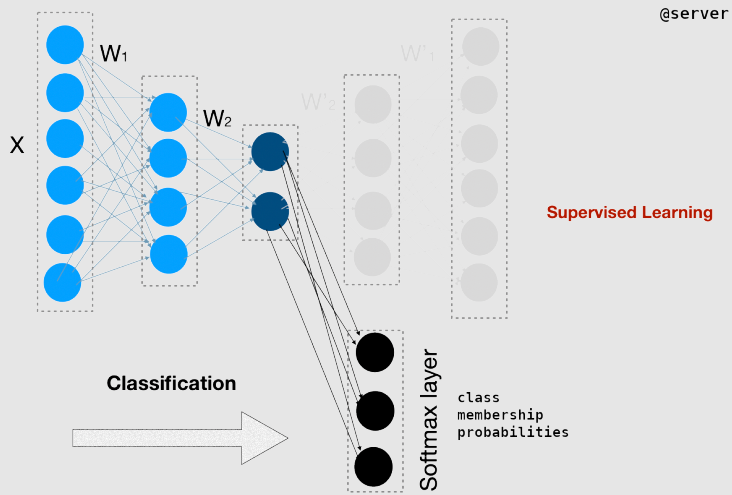


FLuIDS



FLuIDS

Split-Learning



## Dataset IIoT

| | |
|---|---|
| Nb input variables | 197 |
| Nb output variables | 1 |
| Training set | 175,341 |
| Unlabeled set | 122,739 |
| Labeled set | 52,602 |
| Unlabeled ratio | 2.33 |
| Testing set | 82,332 |

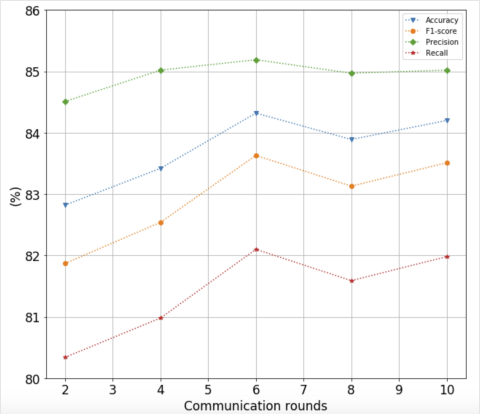
## Federated Learning

| | |
|---|---|
| FL server | 1 |
| Nb clients (Edge devices) | 100 |
| Clients used in federated updates | 10% |
| AE epochs (client) | 5 |
| NN epochs (server) | 20 |
| Communication round | 6 |

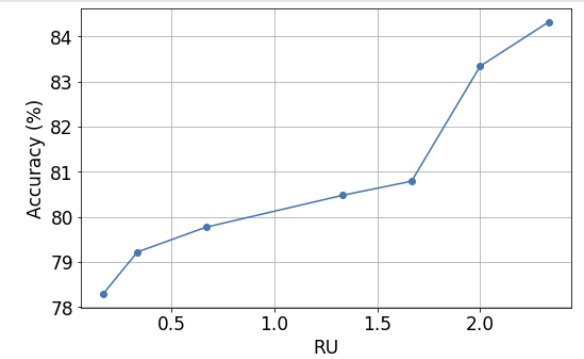
## Deep Learning

| | |
|---|---|
| Deep learning tool | Pytorch |
| DL algorithms | Autoencoder (AE)<br>Neural Network (NN) |
| AE hidden layers | 3 |
| NN layers | 1 |
| Activation functions | Relu (AE), Sigmoid (NN) |
| Optimizer | Adam |
| Learning rate | 0.0001 |
| Batch size | 64 |
| Loss functions | Mean Squared Error (AE)<br>Binary Cross Entropy (NN) |

## Resultats – Nombre de tours

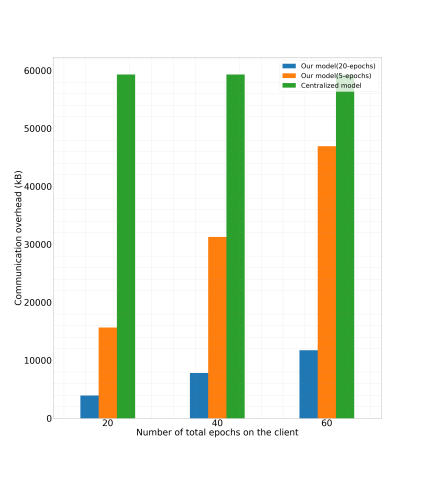


## Resultats – Données non étiquetées

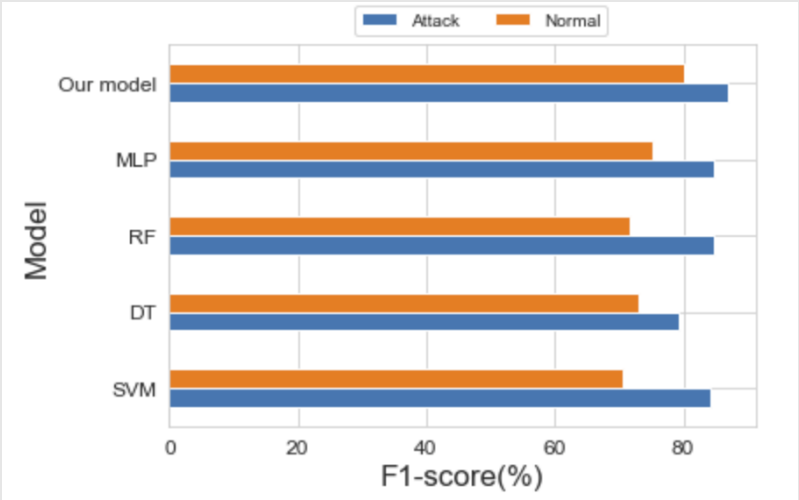



$$R_u = \frac{\#\text{unlabeled}}{\#\text{labeled}} \text{ (\#labeled is fixed)}$$

## Resultat – Surcharge Réseau



## Resultats – Comparaison avec des modèles Supervisés



## Results – Comparaison avec version non-FL

| Model | Accuracy (%) | Precision (%) | Recall (%) | F1-score (%) |
|---|---|---|---|---|
| Non-FL FLuIDS | 81.40 | 83.83 | 79.92 | 80.39 |
| **FLuIDS** | **84.32** | **86.19** | **83.10** | **83.63** |

# Synthèse

## FLuIDS est **semi-supervisé**

- Exploite données **non-étiquetées**
  - *Auto-Encoder + Split Learning*
- Réduit les coûts

## FLuIDS est **fédéré**

- Préserve **confidentialité**
  - *données non déplacées*
- Réduit **charge** serveur
  - *tous les appareils participent*
- Réduit **charge** réseau
  - *taille(mise-à-jour de modèle)* $\lll$ *taille(données brutes)*

# Références


- [Aou+22a] O. Aouedi et al. "Federated Semi-Supervised Learning for Attack Detection in Industrial Internet of Things". In: *IEEE Transactions on Industrial Informatics, SS on Security and Privacy Issues in Industry 4.0 Applications* (2022)
- [Aou+22c] O. Aouedi et al. "Intrusion detection for Softwarized Networks with Semi-supervised Federated Learning". In: *IEEE International Conference on Communications (ICC'22)*. Seoul, South Korea, June 2022
- [Aou+22b] O. Aouedi et al. *FLUIDS: Federated Learning with semi-sUpervised approach for Intrusion Detection System*. Poster at IEEE Consumer Communications and Networking Conference 2022 (CCNC 2022). Virtual Conference, Jan. 2022

# FLuIDS – Perspectives

## Court-terme

- Variational Auto-Encoders
- Fonction d'agrégation

## Moyen-terme

- Few-Shot Learning (Siamese Networks)
- Entraînement sur end-device (TinyML)
  - Alternatives à la BackProp
  - Distribution par couche

# Merci

Merci pour votre attention! ☺

**Questions ?**