Your Connection to ICT Research

CYBER EXCELLENCE research day november 8th

Secure Federated Learning

Xavier Lessage

xavier.lessage@cetic.be

November 8th 2022

www.enmieux.be

FEDER

UNION EUROPEENNE

Wallonie

LE FONDS EUROPÉEN DE DÉVELOPPEMENT RÉGIONAL
ET LA WALLONIE INVESTISSENT DANS VOTRE AVENIR

official partner | digital wallonia .be

Xavier Lessage

Interests

- Artificial Intelligence
- Cloud Computing
- Cybersecurity
- High Performance Computing (distributed data processing)

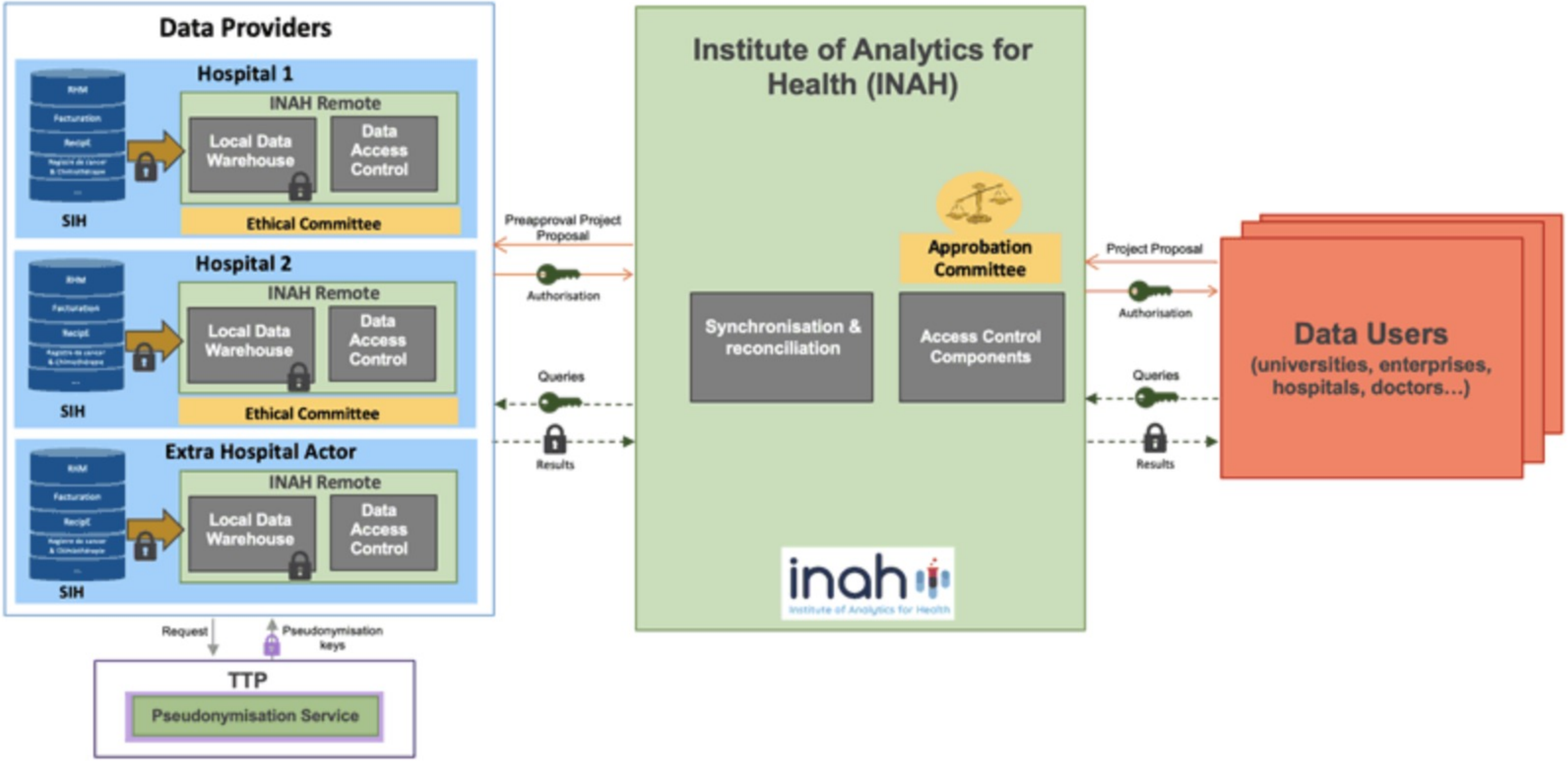
Research topics

- Use of artificial intelligence in healthcare (breast cancer screening, coronary arteries, chest X-ray, ...) with privacy preserving (Federated learning, Homomorphic encryption, ...)
- Deep Learning
  - Architecture (CNN, LSTM, Vision transformers (ViTs), …)
  - Explicability (XAI)
  - Data Augmentation

Research Domain for CETIC :

- Federated Learning (ARIAC Project)
- Homomorphic Encryption
- The Ethical & Secure Platform for Medical Data Analysis (INAH Project)
- Medical Image Analysis

The Ethical & Secure Platform for Medical Data Analysis (INAH Project)



- This platform is designed to enable the ethical and secure use of medical data in statistical and medical research while ensuring the confidentiality of medical data.
- The platform is currently deployed as pilot project within three major Walloon hospitals and also involves local life science companies. It is raising the interest of health actors (e.g., public authorities, universities, pharmaceutical companies.

Federated Learning (ARIAC Project)

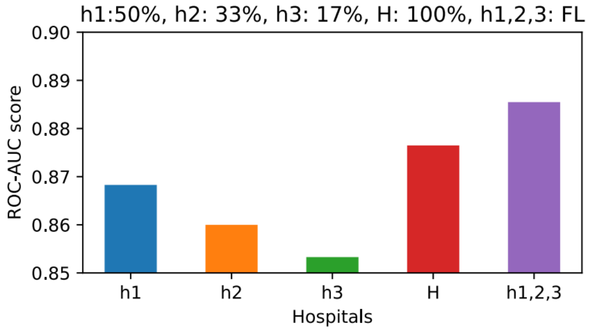
Applications and Research for Trusted Artificial Intelligence (ARIAC)

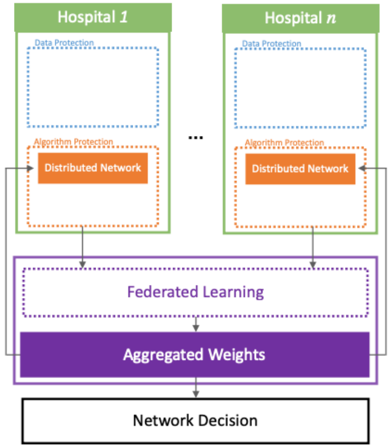
"ARIAC by DigitalWallonia4.ai" is a project bringing together the five French-speaking universities and four Walloon accredited research centres (CRA) to accelerate the development of artificial intelligence technologies in Wallonia.

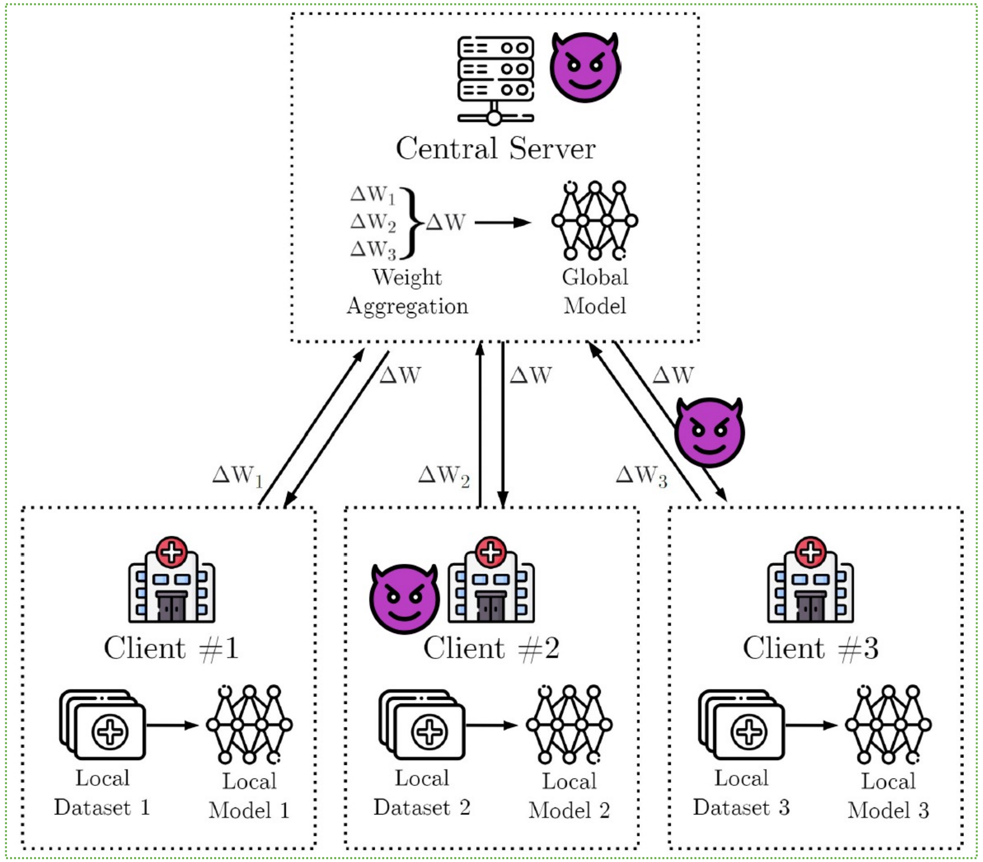
5 Work Package:

- Human-IA interaction
- **Trust mechanisms for AI** (Federated learning, Homomorphic encryption, …)
- Model-IA integration
- Optimised AI implementations
- TRAIL Factory

Final ROC-AUC scores (breast histopathology dataset)







- H shows the score obtain by the single hospital on the entire dataset.
- h1,2,3 shows the score obtained with federated learning.
- h1, h2, h3 shows the score of each hospital when they train solely on their own split.

The Federated Learning paradigm is, because of its nature of decentralized learning, potentially vulnerable to different types of threats and attacks.

Collaborations

In progress

- UCLouvain
  - Equipe de Benoît Marcq
    Federated Learning (Medical Imaging)
  - Equipe de Axel Legay
    Homomorphic Encryption

- UNamur
  - Equipe de Isabelle Vanderlinden
    Federated Recommendation System

- UMons
  - Equipe de Saïd Mahmoudi
    Federated Learning (Medical Imaging)
    Homomorphic Encryption

Area of collaboration sought

- Cryptography for Federated Learning (health and industry sector)
  - Homomorphic Encryption, Classical Encryption (TLS), Secure multi-party computation, etc.

- Analysis of vulnerability to different types of threats and attacks for Federated Learning (health and industry sector)
  - PenTest
  - Inference attacks, Poisonning Attacks

cetic

Your Connection to ICT Research

Aéropole de Charleroi-Gosselies
Avenue Jean Mermoz 28
6041 Charleroi - Belgique

twitter.com/@CETIC 🇫🇷
twitter.com/@CETIC_be 🇬🇧

linkedin.com/company/cetic

info@cetic.be

+32 71 159 362

www.cetic.be