FED-SORAG : Sovereign AI

Federated Sovereign RAG for Secure Knowledge Systems

Project n°10

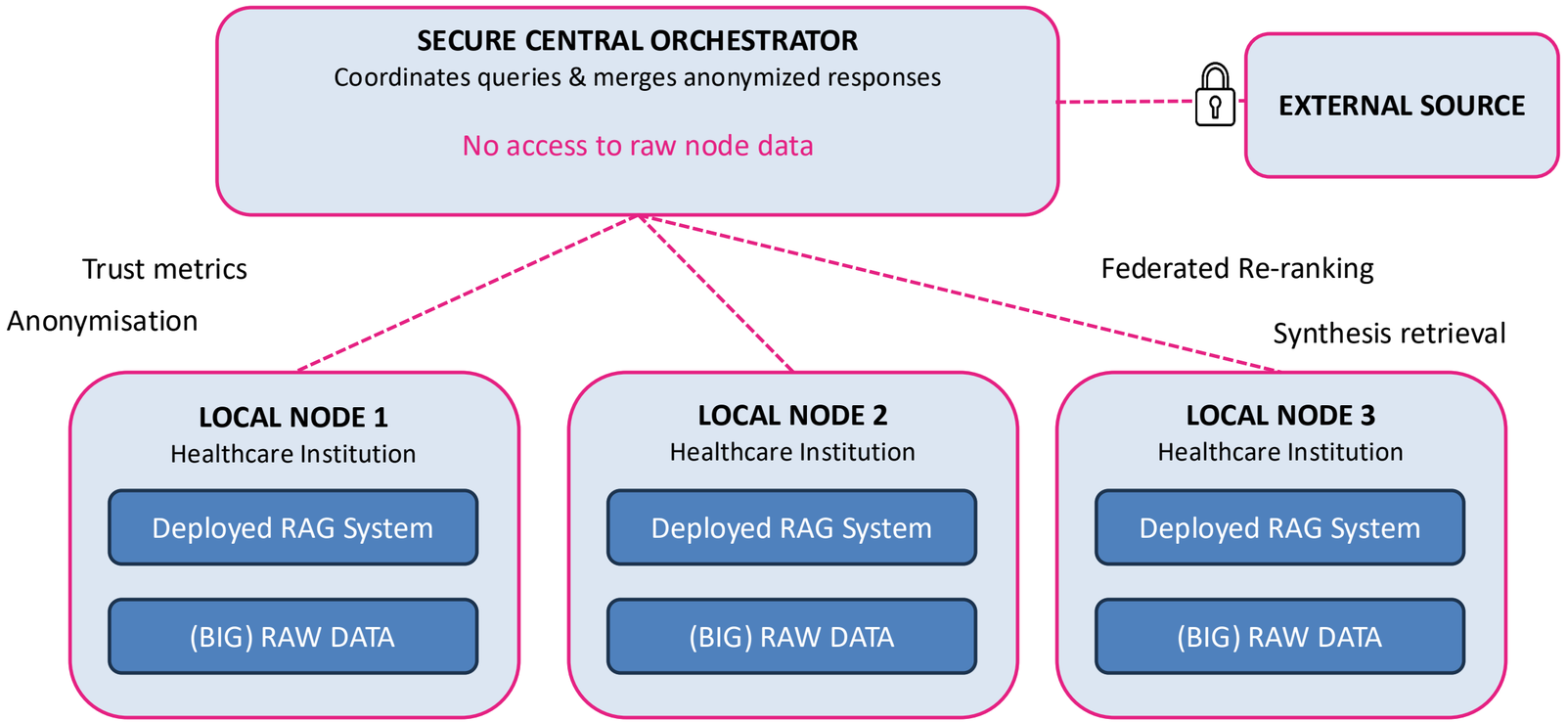
Xavier Lessage (CETIC)

7th TRAIL Research Camp | Lausanne, 2026

01

Context : Sovereign AI

Privacy-Preserving Architecture & Federated Orchestration (FED-SORAG)



KEY PARADIGMS

- **Strict Data Locality**

Zero raw data movement—distributed clinical silos retain 100% data sovereignty.

- **Decentralized Synthesis**

Multi-node response fusion and rank optimization via a global orchestration layer.

Framework Flower.ai (FedRAG Core)

Baseline MIMIC Dataset (FHIR)

TRAIL
TRUSTED AI LABS

02

Founding Team

- *Team Leader 1 : Xavier Lessage*
  - *Institution: CETIC*
  - *Expertise: Secure Federated Learning, LLM, MLOps, …*
- *Team Leader 2 : Christian Colot*
  - *Institution: CETIC*
  - *Expertise: LLM, RAG, …*
- *Team Leader 3 : Raphael Michel*
  - *Institution: CETIC*
  - *Expertise: Federated learning, MLOps, FHIR, …*

TRAIL
TRUSTED AI LABS

03

Work Plan

- *WP1* **Architecture & Core System**
  - *Task 1: Environment Setup & Data Silo Deployment → Establish repositories and deploy simulated clinical data silos using partitioned, FHIR-formatted MIMIC data*
  - *Task 2: Local RAG Node Implementation → Build the ingestion, embedding, and generation pipelines at the node level, including text-to-FHIR bidirectional conversion.*
  - *Task 3: Federated Orchestration & Gateway Routing → Develop the central orchestration layer using Flower for query routing, with a basic gateway for external-knowledge (https://flower.ai/docs/examples/fedrag.html)*

- *WP2 title: Security, Optimization & Evaluation*
  - *Task 1: Adversarial Defense Integration – Implement security layers focusing on prompt injection sanitization, robustness testing against noisy inputs, and content filtering.*
  - *Task 2: Optimization & Structured Retrieval – Fine-tune latency and develop targeted retrieval strategies for specific FHIR resources with unstructured data.*
  - *Task 3 : External Information Retrieval – Augment the quality of the response using external sources as needed in a secure way*

TRAIL
TRUSTED AI LABS

04

Expertise Sought

- ***Research Axis 1 : Federated RAG & Modality Alignment***
  - *Skill 1: Distributed Retrieval & context fusion (Multi-node query routing, Flower framework orchestration, scalable distributed indexing, response ranking & fusion optimization)*
  - *Skill 2: Cross-Modality Representation & Mapping (Heterogeneous data space alignment, structured FHIR/MIMIC resource parsing, text-to-structured conversion, prompt space optimization)*

- ***Research Axis 2 : Adversarial Robustness & Trustworthy AI***
  - *Skill 1: Adversarial ML (Prompt injection defense, node-level query sanitization, …)*
  - *Skill 2: Trustworthy AI Metrics & Governance (Confidence indicators, Provenance tracking, …)*

TRAIL
TRUSTED AI LABS

Unil.

civis

TRAIL

TRUSTED AI LABS

THANK YOU FOR YOUR ATTENTION !

WWW.TRAIL.AC
xavier.lessage@cetic.be

ULB Université Libre de Bruxelles · UMONS University of Mons · UCLouvain · Liège université · Université de Namur · LIEU Liaison Entreprises-Universités · Multitel Innovation Centre · cetic · Cenaero · sirris · S3 · AI4Belgium · digital wallonia .be

Cofinancé par l'Union européenne