AKRAM DIFALLAH

Master of Science Graduate (Networks & ICT) | Ph.D. Candidate in Trustworthy AI & AI Systems

Tolga, Biskra 07001, Algeria • akrammdifallah@gmail.com • +213 6 57 76 51 62 • github.com/dlfallah • Algerian

RESEARCH OBJECTIVE & ABSTRACT PROFILE

M.Sc. Graduate in Networks & Information Technologies pursuing a Ph.D. in **Trustworthy AI, Privacy-Preserving Machine Learning (PPML), and Healthcare Edge-IoT**. Credentialed clinical researcher (PhysioNet) certified in human subjects research (CITI Program). Combines Conformal Risk Control, Homomorphic Encryption (CKKS), and Federated Learning with advanced **AI Engineering**—including Specification-Driven Development (SDD), Context Engineering, and RAG-driven autonomous clinical assistants.

EDUCATION & SCIENTIFIC CREDENTIALS

Master of Science (M.Sc.) in Networks & ICT (RTIC) — Graduated **2024 – 2026**
University of Mohamed Khider, Biskra, Algeria — High Honors (Top of Promotion)

Bachelor of Science (B.Sc.) in Computer Systems (Licence Informatique) **2021 – 2025**
University of Mohamed Khider, Biskra, Algeria — Honors

Clinical Credentials: **PhysioNet Credentialed Researcher** (MIMIC-IV, eICU-CRD databases); **CITI Program Certification** (Human Subjects Research, Biomedical Data Privacy & GCP Ethics).

Languages: **French:** Level B2 (Official TCF SO Score: **403**) • **English:** Professional Research Proficiency (B2/C1).

TECHNICAL STACK & AI ENGINEERING COMPETENCIES

AI Engineering & LLMs: **Specification-Driven Development (SDD)**, **Context Engineering** (sliding token buffers, dynamic injection), **Prompt Engineering** (few-shot, CoT, structured schemas), **RAG** (hybrid BM25/vector retrieval, reranking), **Autonomous AI Assistants** (tool calling, schema validation).

PPML & Cryptography: Homomorphic Encryption (CKKS & BFV via TenSEAL, SEAL), Conformal Risk Control (CRC, MAPIE), Federated Learning (Flower/Flwr, FedProx), Differential Privacy (DP-SGD, Rényi DP, Opacus), Secure Aggregation.

Systems & Languages: Python (PyTorch, NumPy, SciPy, FastAPI), C/C++, Java (Spring Boot), SQL (PostgreSQL, SQLite WAL), Linux/Bash, Docker, MQTT (Mosquitto), Git, LaTeX/BibTeX.

CORE RESEARCH & ENGINEERING MODULES

- **1. Distribution-Free Conformal Risk Calibration (PyTorch, MAPIE, SDD):** Formulated Split Conformal Risk Control (CRC) providing finite-sample coverage guarantees on physiological deterioration predictions. Formulated SDD deterministic test suites bounding clinical risk below error threshold $\alpha = 0.05$ under covariate shift.
- **2. Encrypted Neural Inference via CKKS Homomorphic Encryption (TenSEAL, SEAL):** Designed zero-knowledge inference pipeline over encrypted patient vitals using CKKS arithmetic scheme. Parameterized $N = 8192$ with 128-bit post-quantum security; constructed low-degree Chebyshev polynomial activations to manage noise budget.
- **3. Federated Anomaly Detection for Ambulance IoT (Flower, FedProx):** Engineered decentralized multi-client federated network across mobile ambulance nodes detecting ECG/SpO2 multivariate anomalies without centralizing raw data. Deployed FedProx to neutralize non-IID statistical drift and intermittent connectivity.
- **4. Differentially Private Secure Aggregation (DP-SGD, Opacus, Rényi DP):** Combined client-side gradient clipping and calibrated Gaussian noise tracked via Rényi DP with pairwise additive secret masking, shielding distributed healthcare updates against gradient inversion and membership inference attacks.
- **5. Clinical RAG AI Assistant & Resilient Edge Telemetry (MQTT, SQLite WAL, RAG, SDD):** Implemented an offline-tolerant edge telemetry ingestion buffer (SQLite WAL / QoS-2 MQTT) and paired it with a RAG-powered **Autonomous Clinical AI Assistant** using context engineering and strict SDD schema enforcement for triage summaries.

INDUSTRIAL EXPERIENCE

Technical Engineering Intern — Integrated Control & Safety Systems (ICSS) **Mar 2025 – Apr 2025**
Sonatrach DP Hamra — Industrial SCADA, DCS, SIL3 safety architectures, and Modbus/TCP network segregation.