Fellow	Roufaida **Laidi**
Host Organisation	NTNU, Norway
Scientific coordinator	Ilangko **Balasingham**

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

During my fellowship, I focused primarily on **federated learning (FL)** techniques, a type of distributed learning that allows multiple sites (e.g., hospitals) to train models collaboratively without directly sharing sensitive data, thus aligning with data-privacy regulations such as the GDPR. Specifically:

- **Personalized FL Approaches:** I explored methods to reduce data heterogeneity by generating synthetic data to balance distributions among different clients using **generative AI** (including diffusion models). This ensured that each site could benefit from a more robust global model without compromising data privacy.
- **Trade-offs in FL Systems:** I investigated strategies to balance **privacy, model performance, and resource efficiency** in FL for IoT networks. These efforts included applying differential privacy techniques for robust privacy guarantees and analyzing the impact of network constraints on model training.
- **Collaborations:** Although I did not have on-site AI collaborators at my host institution NTNU, I worked remotely with colleagues at Oslo University Hospital, who provided expertise in handling medical data with AI models.

Overall, my work aimed at enabling higher-quality, personalized FL models while mitigating data skewness and maintaining strong privacy protections.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

Accepted/Published Work

1. Federated Learning in IoT Environments: Examining the Three-way See-saw for Privacy, Model-Performance, and Network-Efficiency
    - Publication Status: Accepted in IEEE Communications Surveys & Tutorials
    - Abstract (abridged): This survey explores privacy-preserving techniques in FL for IoT and their impact on model performance and network efficiency. We introduce a customized taxonomy evaluating privacy, QoS, and network efficiency in various PPFL solutions, highlighting their interplay and discussing real-world industrial case studies. The findings underscore that no single PPFL technique fits all IoT scenarios, identifying key directions for future research in next-generation networks.
2. TG-SPRED: Temporal Graph for Sensorial Data PREDiction
    - Authors: R. Laidi, D. Djenouri, Y. Djenouri, J. Chun-Wei Lin
    - Journal: ACM Transactions on Sensor Networks (In Press, May 2024)
    - Abstract (abridged): Introduces TG-SPRED, a model designed to minimize energy consumption in sensor networks by predicting sensor data. It combines Gated Recurrent Units and Graph Convolutional Networks, improving both accuracy and energy efficiency compared to six leading solutions.
3. Generating Event Sensor Readings Using Spatial Correlations and a Graph Sensor Adversarial Model for Energy Saving in IoT: GSAVES
    - Authors: R. Laidi, D. Djenouri, M. Bagaa, L. Khelladi, Y. Djenouri
    - Conference: IEEE PIMRC 2023 (Toronto, Canada)
    - DOI: 10.1109/PIMRC56721.2023.10293922

- Abstract (abridged): Proposes GSAVES, which utilizes graph convolutional networks to generate missing sensor data, reducing energy consumption in IoT networks. The approach outperforms state-of-the-art solutions in striking a balance between energy efficiency and accuracy.

In Preparation / Pending

4. Generative Models in Federated Learning: Addressing Data Heterogeneity and Privacy Concerns
    - Target Venue: IEEE Network Magazine
    - Abstract (abridged): This manuscript delves into how generative AI (GANs, VAEs, diffusion models) can address data skewness in FL frameworks while preserving privacy. By creating synthetic data that balances local distributions, we improve model robustness and performance. The paper concludes with proposed directions for integrating generative AI into FL systems more effectively.

In addition to these publications, I also contributed to **grant proposals** related to federated learning and data privacy.

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

Autumn Research School in AI Methods in Medical Imaging (September 2023, Sommarøy, Norway)
Organized by PRESIMAL and the Norwegian Artificial Intelligence Research Consortium (NORA), this school provided hands-on sessions and lectures on deep learning pipelines in medical imaging.

- *Presentation*: Poster titled "Enhancing Medical Image Segmentation in Federated Learning: Addressing Data Heterogeneity through Node-Specific Fine-Tuning." This work showcased an approach to personalize FL models for medical imaging data via locally fine-tuned layers.

Workshops Organized

1. Industrial Workshop – "Securing the Future of Medicine: Solutions for AI and IoT Privacy and Safety"
    - Date/Location: November 7, 2024, Health2B (Oslo, Norway)
    - Description: Brought together industry leaders and academics to discuss cutting-edge research and practical challenges at the intersection of AI, IoT, and healthcare cybersecurity.
2. Healthcare Data Privacy Webinar (CybAlliance Project)
    - Date/Location: April 7, 2025 (Online)
    - Description: Co-organized a webinar assembling experts from academia and industry to address regulatory compliance, privacy-preserving technologies, and AI-driven security risks in healthcare.

IV – RESEARCH EXCHANGE PROGRAMME (REP)

I conducted my REP at **The Institute of Software Engineering and Technologies (ITIS), Málaga, Spain** with the ERTIS Research group, from **4–15 December**. My local contacts were **Prof. Manuel Díaz Rodríguez** and **Dr. Cristian Martín Fernández**. This exchange allowed me to see firsthand how an IoT-focused research group closely collaborates with industry partners to translate research into real-world applications. I gained insights into practical challenges of deploying FL at industrial scales, reinforcing the importance of resource optimization and robust privacy frameworks.

V – SUM UP OF THE FINAL SCIENTIFIC REPORT FOR THE ERCIM NEWSLETTER

Dr. Roufaida Laidi has spent her ERCIM fellowship at NTNU focusing on federated learning and generative AI, tackling data heterogeneity and privacy concerns in distributed medical and IoT contexts. During her stay, she developed methods that balance privacy, resource efficiency, and learning performance, culminating in a high-impact survey in IEEE Communications Surveys & Tutorials. She will continue this research as she joins Oslo University Hospital, aiming to further integrate FL into practical healthcare solutions. You can reach her at ar_laidi@esi.dz.