Fabiola Espinoza Castellon

47 Av du Président Allende, Massy, 91300
(+33) 7 83 78 81 24
fabiola.espinoza.castellon@gmail.com
Bolivian and Nicaraguan

Education

2020–present **Ph.D., Computer Science**, *Université Paris-Saclay*, Saclay, France.
Ph.D. under the supervision of Cédric Gouy-Pailler and Aurélien Mayoue. Publications in international conferences and teaching assistantships for undergraduate and graduate levels.

2017–2020 **M.Eng specialized in Artificial Intelligence**, *Telecom SudParis*, Evry, France.
Master's Engineering degree specialized in AI. Joint specialization with Telecom Paris and ENSTA Paris.

2015–2017 **Preparatory classes in Maths/Physics section**, *Lycée Thiers*, Marseille, France.
Preparation for competitive entrance exams to leading French engineering schools.

Experience

Nov 2020 – present **PhD, Computer Science**, *CEA List*, Saclay, France.
Ph.D. entitled "Contributions to effective and secure federated learning with client data heterogeneity".
Keywords: federated learning, data heterogeneity, backdoor attacks, robustness, machine learning.

Apr 2020 – Oct 2020 **End of studies internship**, *EDF R&D*, Saclay, France.
- Wind power forecast using deep learning techniques.
- Programming done in Python using tensorflow/keras.

Jul 2019 – Sep 2019 **Summer internship**, *United Nations Pulse Lab*, Jakarta, Indonesia.
- Estimation of electrification and energy consumption in Indonesia
- Used remote sensing data (night-time satellite imagery), ground truth data (official statistics) and open data.
- Analysis done in Python (pandas, GDAL) and ArqGIS.

Academic achievements and recognitions

2015 – 2020 **Bourse Excellence-Major**, scholarship (2015-2020) awarded to non-French students in French schools outside France based on high school academic excellence. 14 awards in all Latin America.

2023 **Best Paper Award**, "FUBA: Federated Uncovering of Backdoor Attacks" at 2023 IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications.

2024 **G-Research quantitative research grant**, Grant for early career researchers, awarded to enable innovative research in a quantitative discipline.

Presentations

Incremental clustering for federated learning with heterogenous data

May 2022 **Plateau de Saclay's ICST doctoral students' day**, *Université Paris Saclay*, poster presentation.

Jun 2022 **Groupe de recherche (research group) on distributed and federated AI**, *CNRS - Sorbonne Université*, presentation.

Jul 2022 **WCCI IEEE World Congress on Computational Intelligence 2022**, *Padova, Italy*, poster.

Jan 2023 **Workshop FL-Day - Decentralized Federated Learning: Approaches and Challenges**, *DATAIA Institute of Paris-Saclay*, poster.

Training-time poisoning attacks in federated learning

Mar 2023 **GT (groupe de travail) on cybersecurity**, *Hub France IA*, presentation.

Sep 2023 **Colloque GRETSI**, *Grenoble, France*, poster.

Nov 2023 **IEEE TPS-ISA**, *Atlanta, US*, presentation.

Services

Jul 2022 Chair of the Applications in Health Care workshop. **WCCI IEEE World Congress on Computational Intelligence 2022**, *Padova, Italy*.

Mar 2024 Reviewer. **Multimedia Tools and Applications, Springer**.

Publications

In International Conference Proceedings

2024 Fabiola Espinoza Castellon, Eduardo Fernandes Montesuma, Fred Ngolè Mboula, Aurélien Mayoue, Antoine Souloumiac, and Cédric Gouy-Pallier. Federated dataset dictionary learning for multi-source domain adaptation. In *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2024.

2023 Fabiola Espinoza Castellon, Aurélien Mayoue, Deepika Singh, and Cédric Gouy-Pailler. Fuba: Federated uncovering of backdoor attacks for heterogeneous data. In *International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE, 2023. **"Best Paper Award"**.

2022 Fabiola Espinoza Castellon, Aurélien Mayoue, Jacques-Henri Sublemontier, and Cédric Gouy-Pailler. Federated learning with incremental clustering for heterogeneous data. In *2022 International Joint Conference on Neural Networks (IJCNN)*, pages 1–8, 2022.

In National Conference Proceedings

2023 Fabiola Espinoza Castellon, Deepika Singh, Aurélien Mayoue, and Cédric Gouy-Pailler. Défense contre les attaques par porte dérobée en apprentissage fédéré par estimation du motif d'attaque et élagage. In *Groupe de Recherche et d'Etudes de Traitement du Signal et des Images*, 2023.

Teaching

Feb 2021 & Feb 2023 **INSTN (Institut National des Sciences et Techniques Nucléaires)**, Saclay, France.
- AI Unit for Master 2 Embedded Systems and Information Processing.

Jan 2022 & Jan 2023 **Telecom SudParis**, Evry, France.
- Statistical modeling and applications Unit for 3^{rd} year students (Master 2 equivalent).

Sep 2021 – Apr 2022 **IUT de Sceaux**, Sceaux, France.
- Statistics for two-year technical degree (IUT) students in Marketing techniques (L1).

Skills

Projects PYTHON, PyTorch, LaTeX, Git, Bash, GPU allocation, Slurm (workload manager)

Languages

Fluent Spanish (mother-tongue), French, English

Advanced Portuguese

Interests

Volunteering English tutor (AIESEC Brazil), transitional housing (TECHO Bolivia, Brazil, Nicaragua).

Leisure & sports Swimming, running, workout, traveling (America, Africa, Europe and Asia).