

# Jonas Ngnawé

Quebec City, Canada

✉ ngnawejonas@gmail.com • 🌐 ngnawejonas.github.io • in jonasngnawe  
Google Scholar • Stanford Profile

## Education

<b>Université Laval (IID), Mila - Quebec AI Institute, Stanford (VSR, 2025-2026)</b> <i>PhD in Computer Science: Adversarial Machine Learning</i>	<b>Quebec, Canada</b> 2021–2026
<b>AIMS African Master's of Machine Intelligence</b> <i>MSc in Machine Learning</i> Funded by Meta and Google; taught by world top researchers.	<b>Kigali, Rwanda</b> 2018–2019
<b>African Institute for Mathematical Sciences (AIMS)</b> <i>MSc in Mathematical Sciences</i>	<b>Limbe, Cameroon</b> 2016–2017
<b>École Polytechnique</b> <i>MSc in Computer Engineering</i>	<b>Yaoundé, Cameroon</b> 2011–2016
<b>Summer Schools:</b> Machine Learning Summer School (MLSS), London 2019; Deep Learning & Reinforcement Learning Summer School (DLRL), Edmonton 2025.	

## Publications

Detecting Brittle Decisions for Free: Leveraging Margin Consistency in Deep Robust Classifiers, **Ngnawé, J.**, Sahoo, S., Pequignot, Y., Précioso, F., & Gagné, C. (NeurIPS 2024). [NeurIPS Proceedings]

A Layer Selection Approach to Test Time Adaptation, Sahoo, S., ElAraby, M., **Ngnawé, J.**, Pequignot, Y., Précioso, F., & Gagné, C. (AAAI 2025). [AAAI Proceedings]

Robust Fine-Tuning from Non-Robust Pretrained Models: Mitigating Suboptimal Transfer with Adversarial Scheduling, **Ngnawé, J.**, Heuillet, M., Sahoo, S., Pequignot, Y., Ahmad, O., Durand, A., Précioso, F., & Gagné, C. (NeurIPS 2025 Workshop on Reliable ML). [arXiv]

A Guide to Robust Generalization: The Impact of Architecture, Pre-training, and Optimization Strategy, Heuillet, M., Bhagwatkar, R., **Ngnawé, J.**, Pequignot, Y., Larouche, A., Gagné, C., Rish, I., Ahmad, O., & Durand, A. (NeurIPS 2025 Workshop on Reliable ML). [arXiv]

Robustmix: Improving Robustness by Regularizing the Frequency Bias of Deep Networks, **Ngnawé, J.**, Njifon, M. A., Heek, J., & Dauphin, Y. (NeurIPS 2022 Workshop on Distribution Shifts). [OpenReview]

Scalable Inference with Distributed Gaussian Processes using the Wasserstein Barycenter, **Ngnawé, J.**, Deisenroth, M. (Master's project). [GitHub]

k-Clustering Problem: Application to a Field Technician Allocation Optimization Problem, **Ngnawé, J.**, Zacko, E., Wandji, N., & Ndjinga, M. (Master's project). [ResearchGate]

## AI/ML Work Experience

<b>Stanford Artificial Intelligence Lab (SAIL)</b> <i>Visiting Student Researcher</i> ○ Adversarial robustness of Vision-Language Models. ○ AI Measurement Science applied to LLMs Evaluation	<b>Palo Alto, USA</b> Oct 2021 – to Date
<b>Google Brain</b> <i>Google AI Resident</i> ○ Development of robust methods for deep neural networks. ○ Compression of deep neural networks by quantization and pruning.	<b>Accra, Ghana</b> Oct 2019 – Sep 2021

## Other Work Experience

---

### GroupOne Holding Company

Computer Engineer

Limbe, Cameroon

Jan – Aug 2018

- Website development; fuel consumption prediction projects.
- Studies for the creation of a startup incubator (business plan).
- Industrial maintenance (refinery) of the Honeywell Experion System; IT support.

**Tools:** HTML5/CSS3/JavaScript/jQuery/jQueryUI/Ajax/PHP, MySQL, PMI Methodology, Business Model Canvas.

Cameroon

Freelance Software Developer

2017–2018

- Digitization of administrative procedures for various ministries in Cameroon.
- Development and maintenance of WordPress plugins (WooCommerce).

**Tools:** DevOps, Electronic Document Management (EDM)/Electronic Archiving (Maarch RM), PHP, WooCommerce, MySQL Workbench, Microsoft Access, Git/GitLab/GitHub, Java, NetBeans, SCRUM.

### Bolloré Africa Logistics

Douala, Cameroon

Software Developer Intern

Feb – Aug 2016

- Automation and analysis of the review of access rights to the Information System.
- Detection of abnormal access rights.

**Tools:** Talend Open Studio, QlikView, C#, ASP.NET, Microsoft SQL Server, Visual Studio, UML/Merise, BPMN 2.0, PMI Methodology.

## Talks

---

Host at Kmer AI Talks.

**2024:** Panelist, “AI Regulation & Fairness in the Generative AI Era,” Black in AI Workshop @ NeurIPS.

**2024–2025:** “Detecting Brittle Decisions for Free” — Kmer AI (Jun 2024); Galsen AI (Jan 2025).

**2022:** Keynote, “Robustness in AI,” Deep Learning IndabaX-Cameroon (Dec 27, 2022).

## Reviews

---

NeurIPS 2025; IEEE Transactions on Image Processing.

Algorithmic Fairness workshops @ NeurIPS 2021, 2022, 2023, 2024.

Montreal AI Symposium (2022, 2024); Black in AI Workshop (2022–2024).

Deep Learning Indaba, Pan-African Machine Learning Conference (2023).

## Leadership & Event Organization

---

Organizing committee: Interpolate Workshop @ NeurIPS 2022 (First Workshop on Interpolation Regularizers and Beyond).

Co-organizer: Machine Learning Projects Competition (MLPC) 2020–2022, Polytechnique Yaoundé.

Co-organizer: Two-week introductory course in Machine Learning (Sep 2019), Polytechnique Yaoundé.

Co-organizer: First Deep Learning IndabaX Rwanda (Apr 2019), Kigali, Rwanda.

Co-Founder of Kmer-AI, an association for promoting and popularizing AI and ML in Cameroon (since 2020).

## AI/ML Skills

---

**ML Frameworks:** PyTorch, TensorFlow, Scikit-Learn

**MLOps Tools:** Git/GitHub, Weights & Biases, Docker, Ray, Slurm, Google Cloud Platform

**Other:** Distributed Training, VLMs/LLMs, Adversarial Evaluation