Hanan Ather

Member of Technical Staff | Adversarial ML, Privacy & Security

hananather.com | hathe098@gmail.com | linkedin.com/in/hanan-ather | github.com/hananather

Education

University of Ottawa — Ottawa, Canada

Master of Science in Mathematics and Statistics, Concentration in Statistics — *2021 – 2024*

- Thesis: Deep Reinforcement Learning & Function Optimization; completed while working full-time.

University of Ottawa — Ottawa, Canada

Honours B.Sc. — Mathematics & Statistics, ***Dean's Honours List*** — *2015 – 2020*

Experience

Centre for AI Research and Excellence, Statistics Canada — Ottawa, Canada

Member of Technical Staff | JAX, Pytorch, Ray, XLA/MLIR — *April 2025 – Present*

- Won International Association for Official Statistics Young Statisticians Prize 2025 for Bayesian framework integrating LLMs with calibrated uncertainty; reduced manual review by 50% while preserving human-in-the-loop safeguards.
- Built evaluation framework for membership inference, data leakage, and reconstruction attacks for production; developed mitigations including DP fine-tuning, federated learning, and constitutional filters.
- Authored security frameworks for AI systems on confidential data; mapped attack surface (prompt injection, extraction, MIA, poisoning) and designed layered mitigations.
- Member of Office of Responsible AI; Lead technical reviews of AI systems across government; contributed to Agentic AI frameworks and governance guidance to international bodies (UNECE, G7 GovAI, Mila, ISI).

Statistics Canada — Ottawa, Canada

AI Research Engineer | Python, Apache Arrow, DuckDB, LangGraph, Pydantic — *March 2024 – April 2025*

- Deployed production RAG system extracting unstructured data from millions of records; integrated guardrails for safe automation, reducing analyst overhead by 85%.
- Designed **LLM fine-tuning** (**QLoRA, LoRA**) pipeline for cost-effective domain-specific model adaptations on GPU clusters reducing memory requirements by **63%**.
- Built a containerized hierarchical classification pipeline for NAICS codes using LoRA-finetuned LLMs, categorizing 8M+ Canadian businesses in real time across 2,300+ categories.

Statistics Canada — Ottawa, Canada

Data Scientist | Python, SQL, Spark, Airflow, dbt — *July 2022 – March 2024*

- Architected and deployed a **distributed data integration** pipeline across multi-cloud environments (AWS/GCP/Azure). Processed **1B+ monthly rows**, cutting runtime from days to hours.
- Led the design and implementation of a **CI/CD-enabled data pipeline**, reducing cost by over 80% (measured by hours of manual work)

Treasury Board of Canada Secretariat — Ottawa, Canada

Data Scientist | Python, SQL, TypeScript/JavaScript — *December 2020 – July 2022*

- Engineered **CI/CD automated workflows** in Python, integrated with GitHub Actions for daily batch jobs, eliminating 2 weeks of manual processes per fiscal year and improving operational monitoring.
- Fine-tuned a **BERT-based semantic search** pipeline on thousands of government audit comments, enabling real-time topic clustering and sentiment analysis for 35+ departmental heads.
- Developed and deployed a **production-grade full-stack risk assessment system** (FastAPI + React) for federal auditors, automating data ingestion, real-time inference, and interactive dashboards for enterprise risk analysis.

Technical Skills

ML & Research: Python (9+ yrs), PyTorch, JAX, TensorFlow, model fine-tuning, distributed training, experiment tracking, empirical ML research

Security: Red teaming, vulnerability research, threat modeling, adversarial evaluation, fuzzing, code security review, penetration testing

Infrastructure: GCP, AWS, Docker, Kubernetes, CI/CD, open-source development