

Kaysarul Anas

✉ kaysarulanas2@gmail.com | 📞 +1 (249) 979-3459 | 🌐 research.kaysarulanas.me | 📄 github.com/anaskaysar

📍 Canada

Applied ML & LLM · Full Stack Developer (Python & React)

Objective

M.Sc. graduate in Computational Sciences with production experience in backend development, cloud infrastructure, and CI/CD automation on AWS. Active researcher in LLM security and adversarial ML with two papers under review; seeking a Software Engineering or AI/ML Engineering role.

Relevant Experience

Contract AI Research Engineer | Nexirion / Laurentian University May 2025 – Present

- **Multi-Agent Architectures:** Designed a 3-tier multi-agent RAG pipeline for network intrusion detection over the CIC-UNSW-NB15 corpus (3.54M flows, 10 attack classes); deployed and evaluated the detection tier end-to-end, outperforming tree-based ML baselines by 30%+ F1 on select low-prevalence attack classes.
- **Adversarial Defense:** Designed and implemented a retrieval-boundary defense (trust scoring, label-embedding consistency checking, prompt sanitization) that recovered up to 100% of clean-baseline F1 under 1% knowledge-base poisoning and held multi-document prompt-injection success below 2.4%, adding under 5ms of latency overhead per query.
- **RAG Optimization:** Deployed a 4-bit quantized 7B-parameter LLM via bitsandbytes on a single 16GB GPU, engineering a hybrid dense+sparse (BGE-M3 + BM25, reciprocal rank fusion) retrieval pipeline for real-time classification under strict memory constraints.

Junior Software Engineer (R&D) | MyCell Technology Limited, Dhaka, Bangladesh Jul 2022 – Jun 2023

- Architected and deployed scalable, production-grade microservices and backend features using Python and full-stack frameworks.
- Analyzed existing monolithic systems to optimize performance, integrate modern tech stacks, and drive technical direction during company engineering sprints.

Software Engineering Intern | MyCell Technology Limited, Dhaka, Bangladesh Jan 2022 – Jun 2022

- Developed user-facing features for responsive production web applications using React, JavaScript, and modern front-end libraries.
- Engineered internal data analysis scripts using Pandas, NumPy, and TensorFlow to process and clean production datasets.

Undergraduate Research Assistant | TNR Lab, North South University, Bangladesh May 2022 – Apr 2023

Supervisor: Dr. Tanzilur Rahman (Assistant Professor, KFUPM, Saudi Arabia)

- Led medical image analysis pipeline for pulmonary fibrosis prediction using EfficientNet and Quantile Regression; co-authored and presented at **IEEE TENSYP 2023**, Canberra, Australia.

Education

Laurentian University, Sudbury, ON, Canada Sept 2023 – Apr 2025

M.Sc. in Computational Sciences

CGPA: 9.10 / 10.00

- **Award:** Mabel Jean and Bob Lye Memorial Award for Academic Excellence (\$2,000), 2024–2025.
- **Coursework:** Advanced ML/Deep Learning, AI/ML in Cybersecurity, Applied Cryptography, Ethical Hacking, Image Processing & Computer Vision, Autonomous Mobile Robotics.

North South University, Dhaka, Bangladesh

Jan 2018 – Aug 2022

B.Sc. in Computer Science & Engineering

CGPA: 3.40 / 4.00

- **Key Courses:** Natural Language Processing, Machine Learning, Data Structure and Algorithms, Database System, Software Engineering Fundamentals.
- Innovation Challenge Season 11 — Top 10 of 80 teams (technical evaluation & presentation).

Technical Skills

Languages:	Python, JavaScript (ES6+), SQL (PostgreSQL, MySQL), Bash
ML & Deep Learning:	PyTorch, TensorFlow, scikit-learn, OpenCV, YOLO, Computer Vision, Deep Learning
LLM & NLP:	RAG Pipelines, LangChain, Hugging Face Transformers, Vector Databases, Prompt Engineering, BM25, RAGAS
Backend Development:	Django, Flask, FastAPI, Node.js, REST APIs, JWT Authentication
Frontend:	React , Next.js, Tailwind CSS
Cloud & DevOps:	AWS (EC2, S3), GCP, Docker, GitHub Actions, CI/CD
Tools:	Git/GitHub, Linux, Jupyter, Postman, Latex, Hugging Face Spaces
Research Domains:	LLM Security, Retrieval Poisoning, Adversarial RAG, Post-Quantum Cryptography, Medical Image Analysis, Information Retrieval, Explainable AI

Research & Projects

Adversarial RAG-IDS | Architected & Led · Secure RAG-Based Intrusion Detection 2026 – Present
Collaborating with Dr. Sk. Md. Mizanur Rahman (Centennial College / Laurentian University)

- **Designed** a secure multi-agent RAG architecture for intrusion detection with retrieval-layer defenses including trust scoring, semantic anomaly detection, and prompt sanitization.
- **Leading** evaluation against Random Forest, XGBoost, and LSTM baselines on UNSW-NB15 and CIC-UNSW-NB15 datasets. Targeting **IEEE CIC 2026** with planned extension to **IEEE TDSC**.

BioReactPi | Engineered & Built · Edge AI Bioreactor Controller 
3rd Place Overall, *CU Hacking 2026, Carleton University, Ottawa*

- Engineered a real-time hardware-software interface running on Raspberry Pi to poll temperature sensors and apply predictive logistic growth mathematical models to forecast biomass fluctuations.

Northern Shift Guard | Architected & Built · AI Shift-Start Screening for Mining Safety   [Live Demo](#)
2nd Place Overall & Best Use of Nemotron (*NVIDIA Brev Credits*), *Cursor Hackathon Sudbury 2026, Laurentian University*

- Built an explainable, zone-aware AI screening tool for Northern Ontario mining operations: GPT-4o vision detects PPE and fatigue cues; a custom zone compliance engine checks results against **Ontario Reg 854** per-zone requirements (surface vs. underground vs. open pit); **NVIDIA Nemotron** generates plain-language prioritized supervisor actions.
- Designed a full audit pipeline persisting every scan (vision JSON, zone verdict, Nemotron action, timestamp) to **TiDB Cloud**; deployed as a single Docker container (FastAPI + React/Vite) with a Render blueprint; fully functional prototype shipped within the hackathon window.

MalariAI - Label-Resilient Decoupled Framework for Universal Cell Segmentation with Explainable Stage Classification [arXiv](#)   [Live Demo](#)

- **Designed and implemented** a two-stage annotation-agnostic framework combining watershed segmentation (75.95% cell recovery on NIH BBBC041) and EfficientNet-B0 with Focal Loss (98.36% classification accuracy).
- Achieved cross-dataset zero-shot validation on MP-IDB (4 *Plasmodium* species, 209 images); deployed as a Flask API on Hugging Face Spaces and submitted for publication to CMIG (Elsevier).

JobTrackerr | Designed, Built & Deployed · Production Full-Stack SaaS Application   [jobtrackerr.com](#)

- Built and deployed a production SaaS platform using Django REST, React, PostgreSQL, and AWS EC2 with JWT/Google OAuth authentication.
- Optimized database queries and indexing, reducing API response times by 30%; automated deployments through CI/CD with Nginx and Gunicorn.

Publications

SciRet: A Compute-Aware Empirical Study of Retrieval and Reranking for Scientific RAG
Kaysarul Anas*, Md Hasibul Hasan *EMNLP 2026* (submitted May 2026, under review).

Accurate Prediction of Pulmonary Fibrosis Progression Using EfficientNet and Quantile Regression
Rofiqul Alam Shehab, **Kaysarul Anas**, Md. Ahsanuzzaman, Tanzilur Rahman* *IEEE TENSYP 2023*, Canberra, Australia.  [doi:10.1109/TENSYP55890.2023.10223673](https://doi.org/10.1109/TENSYP55890.2023.10223673)