Kaysarul Anas Apurba

kaysarulanas2@gmail.com | +1 (249) 979-3459 | research.kaysarulanas.me/
github.com/anaskaysar | Ontario, Canada

M.Sc. Computational Sciences · LLM Security · Adversarial ML · NLP · Explainable AI

Research Interests

Information Retrieval, Large Language Models, Adversarial Robustness, Explainable AI & Medical Image Analysis

Education

Laurentian University, Sudbury, ON, Canada — Sept 2023 – Apr 2025
M.Sc. in Computational Sciences - Course Based — **CGPA: 9.10 / 10.00**

- **Award:** Mabel Jean and Bob Lye Memorial Award for Academic Excellence ($2,000), 2024–2025.
- **Relevant Coursework:** Machine Learning/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**

- **Relevant Coursework:** Machine Learning, Natural Language Processing, Image & Signal Processing, Design & Analysis of Algorithms.
- **Participation:** Innovation Challenge Season 11 — Top 10 of 80 teams (technical evaluation & presentation).

Publications

MalariAI: A Label-Resilient Decoupled Framework for Universal Cell Segmentation and Explainable Stage Classification in Dense Malaria Blood Smears
Kaysarul Anas Apurba, Md Hasibul Hasan, Mohammed Ali, Tanzilur Rahman*
Targeting: Computerized Medical Imaging and Graphics (CMIG), Elsevier. **Status: Manuscript in preparation.**
Preprint will be available on arXiv

SciRet: A Compute-Aware Empirical Study of Retrieval and Reranking for Scientific RAG
Kaysarul Anas Apurba*, Md Hasibul Hasan
Submitted to: EMNLP 2026, May 25, 2026. **Status: Under review (anonymous submission).**

A Non-Invasive Cloud-Based Migration Strategy for Post-Quantum Cybersecurity in Smart HVAC Systems
Mahedee Zaman Moon, **Kaysarul Anas Apurba**, Md Hasibul Hasan, Sk. Md. Mizanur Rahman*
Submitted to: IEEE Symposium on Security and Privacy (S&P) 2027, June 2, 2026. **Status: Under review.**

Accurate Prediction of Pulmonary Fibrosis Progression Using EfficientNet and Quantile Regression: A High Performing Approach
Rofiqul Alam Shehab, **Kaysarul Anas Apurba**, Md. Ahsanuzzaman, Tanzilur Rahman*
IEEE Region 10 Symposium (TENSYMP 2023), Canberra, Australia, September 2023.
doi.org/10.1109/TENSYMP55890.2023.10223673

Ongoing Research

Dependable RAG-Based Intrusion Detection 2026 – Present

Collaborating with: Dr. Sk. Md. Mizanur Rahman (Centennial College / Laurentian University)

- Proposing a secure multi-agent RAG architecture for network intrusion detection with a three-tier Detection–Reasoning–Response pipeline and a dedicated retrieval-layer defense module (trust scoring, semantic outlier detection, prompt sanitization).
- Research questions address: (i) which trust and anomaly mechanisms best resist retrieval poisoning and prompt injection; (ii) how a multi-agent RAG-IDS compares with conventional ML baselines under both clean and adversarial conditions; (iii) the accuracy cost of enabling defenses.
- Planned evaluation on UNSW-NB15 and CIC-UNSW-NB15; baselines include Random Forest, XGBoost, and LSTM; metrics span F1, FPR, RAGAS faithfulness, and false-action rate on benign traffic.
- **Target venue:** Initial submission planned for IEEE CIC 2026, followed by an extended journal version incorporating additional experiments, analysis, and methodological enhancements for submission to IEEE Transactions on Dependable and Secure Computing (TDSC).

Research Experience

First Author & Corresponding Author — SciRet: A Compute-Aware Empirical Study of Retrieval and Reranking for Scientific RAG 2025 – 2026

With: Md Hasibul Hasan (IUBAT)

- Designed and executed a controlled multi-scale evaluation of a fixed scientific RAG pipeline over CORD-19, comparing BM25, BGE-M3 dense retrieval, and RRF hybrid fusion across 1K, 5K, and 15K paper corpora.
- Key finding: hybrid BM25+BGE-M3 retrieval is more robust than either component alone (Recall@10 = 1.000 at 1K and 15K); MS MARCO-trained cross-encoder reranker *reduces* precision on scientific text — a negative result with direct deployment implications.
- Generation faithfulness (RAGAS) improves with corpus scale: 0.917 at 1K to 0.960 at 15K; answer relevancy from 0.680 to 0.870. Engineered GPU memory optimizations enabling stable embedding of 15K documents under compute constraints.
- **Output:** Short paper submitted to **EMNLP 2026** (May 25, 2026, under review). Code, indexes, and evaluation outputs released for replication.
  Code

First — MalariAI (targeting CMIG, Elsevier) 2024 – Present

With: Md Hasibul Hasan (IUBAT), Mohammed Ali (NSU), Tanzilur Rahman† (KFUPM)

- Designed a two-stage decoupled framework addressing three structural failure modes in whole-slide malaria detection: annotation incompleteness in NIH BBBC041, NMS suppression in dense smear regions (58% of images contain cell pairs with IoU > 0.3), and absence of per-cell spatial explainability in any published whole-slide pipeline.
- **Stage 1:** Annotation-agnostic distance-transform guided watershed recovers **75.95% of ground-truth cells** (79.04% centroid-in-box; 82.84% infected-cell sensitivity at IoU ≥ 0.25) on the 120-image NIH BBBC041 test set (5,917 GT boxes) without any annotation input.
- **Stage 2:** EfficientNet-B0 with Focal Loss ($\gamma = 2.0$, per-class inverse-frequency weights) achieves **98.36% overall classification accuracy**; **87.5% and 75.0%** per-class accuracy on rare schizont and gametocyte stages vs. 24.57% and 25.95% AP for Faster R-CNN baseline.
- Grad-CAM++ heatmaps generated per detected cell on full 1600×1200 blood smear images — first whole-slide malaria pipeline with integrated per-cell spatial explainability.
- Cross-dataset zero-shot evaluation on MP-IDB (209 images, 4 *Plasmodium* species, 1,407 infected cells); Stage 1 v2 raises MP-IDB recall from 1.28% to **20.68%** and binary AP from 1.82% to 9.09% without retraining Stage 2.
- **Output:** Manuscript in preparation — targeting *CMIG*, Elsevier.
  Code Demo

Co-author — PQC Migration for Smart HVAC Systems (IEEE S&P 2027) 2025 – 2026

With: Mahedee Zaman Moon (IUT), Md Hasibul Hasan (Laurentian), Sk. Md. Mizanur Rahman (Centennial)*

- Co-authored architecture paper proposing a non-invasive, cloud-based PQC proxy layer for legacy consumer HVAC systems — inserting ML-KEM-768 key encapsulation and ML-DSA-65 authentication between the mobile application and vendor cloud, with zero hardware or firmware modification.
- Contributed to security analysis demonstrating quantum-safe key establishment, per-session forward secrecy, entity authentication, and replay resistance under a quantum-capable adversary model (NIST FIPS 203/204).
- Estimated handshake overhead under 10ms on Raspberry Pi 4; architecture deployable today without hardware replacement or vendor cooperation.
- **Output:** Submitted to **IEEE S&P 2027**, June 2, 2026. Under review.

Undergraduate Research Assistant — TNR Lab, North South University Aug 2022 – Aug 2023

Supervisor: Dr. Tanzilur Rahman (now at KFUPM, Saudi Arabia)

- Led medical image analysis pipeline for pulmonary fibrosis progression prediction using EfficientNet and Quantile Regression; contributed to full pipeline from data preprocessing through model evaluation.
- Co-authored and presented peer-reviewed paper at **IEEE TENSYMP 2023**, Canberra, Australia.

Technical Skills

ML / Deep Learning:	PyTorch, TensorFlow, scikit-learn, OpenCV, EfficientNet, U-Net, Faster R-CNN, Grad-CAM++, Focal Loss, YOLO
NLP / LLM:	RAG pipelines, LangChain, HuggingFace Transformers, Vector Databases, Prompt Engineering, RAGAS, BM25, Cross-encoder reranking
LLM Security:	Retrieval poisoning, prompt injection, adversarial RAG evaluation, trust scoring, semantic anomaly detection
Cryptography / PQC:	Post-Quantum Cryptography (ML-KEM, ML-DSA, FIPS 203/204), AES-256-GCM, RSA-2048
Languages:	Python (primary), JavaScript, SQL (PostgreSQL), Bash
Cloud / DevOps:	GCP, AWS (EC2, S3), Docker, GitHub Actions, CI/CD, Kaggle GPU
Tools:	Git, Linux/Unix, Jupyter, LaTeX, HuggingFace Spaces, Postman

Academic Service & Collaboration

- **Research Network:** Active collaborations with researchers at Laurentian University (Canada), IUBAT (Bangladesh), Centennial College (Canada), IUT (Bangladesh), and King Fahd University of Petroleum & Minerals (Saudi Arabia).

Selected Software Projects

JobTrackerr — Production SaaS job application tracker

- Full-stack platform with Django REST + React (Vite), JWT/Google OAuth, AWS EC2 deployment, Nginx/Gunicorn, CI/CD pipeline. Live at jobtrackerr.com.

EncryptIQ — Interactive cryptography visualization platform

- Live AES-128/256 and RSA-2048 demonstrations with Flask-RESTX backend and React frontend; step-by-step encryption visualizations.