# RIAD AHMED ANONTO

riadahmedanonto355@gmail.com | Google Scholar | riad-ahmed-anonto | Anonto050
anonto-riad.vercel.app

## RESEARCH INTERESTS

Machine Learning | Large Language Models | Computer Security

## WORK EXPERIENCE

### Associate Software Engineer
**Therap BD Ltd.**

Apr 2025 – Present — *Dhaka, Bangladesh*

- Contributed to building and maintaining a standalone **Auth Server**; investigated vulnerabilities and applied principled security fixes.
- Maintained and improved platform-wide **message queues** and **distributed caching** to enhance scalability and reduce latency.
- Implemented passkey-based authentication and replay-attack protections; redesigned application-wide RBAC.

## EDUCATION

### Bachelor of Science in Computer Science & Engineering
**Bangladesh University of Engineering & Technology (BUET)**

February 2020 – March 2025 — *Dhaka, Bangladesh*

**CGPA:** 3.83/4.0
**Notable Courses:** Computer Security | Machine Learning | Computer Networks | Artificial Intelligence | Software Engineering | Data Structures and Algorithms | Object Oriented Programming

### Higher Secondary Certificate
**Notre Dame College**

2017 – 2019 — *Dhaka, Bangladesh*

## RESEARCH EXPERIENCE

### Undergraduate Thesis: Identifying and Addressing User-level Security Concerns in Smart Homes Utilizing "Smaller" LLMs
**Supervisors: Dr. Md. Shohrab Hossain (CSE, BUET), Collaborator: Dr. Suryadipta Majumdar (Concordia University)**

*Accepted at PST 2025 (Acceptance Rate: 26%)* [paper]

- Designed a novel dataset capturing practical security challenges from real-world user concerns in public forums, focusing on smart home IoT security.
- Fine-tuned transformer models, such as **T5** and **Flan-T5**, to build an efficient question-answering system tailored for smart home security.
- Evaluated the framework using metrics like F1 Score, achieving significant improvements in answering domain-specific queries with **89.77% validation improvement**.
- Conducted LDA topic modeling to categorize prevalent security concerns and leveraged synthetic data generation techniques to enhance dataset quality.

### Align Where the Words Look: Cross-Attention-Guided Patch Alignment with Contrastive and Transport Regularization for Bengali Captioning
**Supervisor: Dr. Mohammad Saifur Rahman**

*Submitting at ICPR 2026* [paper]

- Proposed a compute-aware Bengali captioning pipeline combining a frozen **MaxViT** encoder with an **mBART-50** Bengali-native decoder, linked via a lightweight linear+LayerNorm bridge.
- Introduced a novel tri-loss framework: **Patch-Alignment Loss (PAL)** for text-conditioned patch grounding, **InfoNCE** for global discrimination, and **Sinkhorn Optimal Transport (OT)** for fine-grained correspondence.

- Constructed a Bengali-aligned corpus by verifying EN–BN captions with LaBSE and generating **110k bilingual-prompted synthetic images** to augment real MSCOCO pairs.
- Achieved state-of-the-art performance on low-resource benchmarks, improving BLEU-4 (12.29), METEOR (27.98), and BERTScore-F1 (71.20) on Flickr30k-1k, narrowing real–synthetic domain gap by 41%.
- Demonstrated robust cross-domain generalization and compute-efficient training on a single GPU, advancing vision–language alignment for low-resource languages.

### When Safety Blocks Sense: Measuring Semantic Confusion in LLM Refusals

**Supervisor: Dr. Ch. Md. Rakin Haider**

*Planned submission: ACL 2026* [paper]

- Defined semantic confusion: local contradictions where a prompt is rejected while a near-identical neighbor is accepted.
- Built **ParaGuard** (∼10k prompts) with controlled paraphrases to form tight semantic neighborhoods for testing.
- Our token-level **CI/CR/CD** metrics compare each refusal to FAISS-retrieved accepted neighbors using token drift, probability shift, and perplexity contrast—going beyond coarse prompt-embedding cosine.
- Cohort-level analyses across Llama, Mistral, Qwen, and GPT families (and multiple guards) show that **FRR alone isn't sufficient**: systems can have similar FRR yet very different confusion profiles, with our metrics exposing where and why contradictions spike.

### DFCon: Attention-Driven Supervised Contrastive Learning for Robust Deepfake Detection (1st Runners Up, IEEE Signal Processing Cup 2025)

**Supervisor: Dr. Mohammad Saifur Rahman**

*Under Review at ICASSP 2026* [paper]

- Used training data from eight datasets in **DeepFakeBench**, incorporating generative approaches (**diffusion models**, **GANs**, **VAEs**) to create synthetic datasets and train robust detection models.
- Fine-tuned advanced backbones, including **MaxViT**, **CoAtNet**, and **EVA-02**, with **supervised contrastive loss** and focal loss to enhance feature embeddings and classification accuracy.
- Implemented a multi-stage pipeline combining backbone training, classifier fine-tuning, and a majority voting ensemble, achieving **95.83% validation accuracy** and addressing class imbalance effectively.

## ONGOING RESEARCH WORKS

### Leakage at the Boundary: Latent Space Prompt Interpolation Attacks on Public T2I Models

**Supervisor: Dr. Md. Rizwan Parvez (QCRI)**

Ongoing Research (2025 – Present)

- Investigating **latent space interpolation attacks** on diffusion models (e.g., Stable Diffusion, SDXL) to study how banned concepts emerge between safe and unsafe prompts, and benchmarking leakage detection via CLIP, prompt inversion, autoencoders, and human evaluation.

### Visual Backtranslation & Latent-Space Consistency with Patch Alignment for Robust VLMs

**Independent Project**

Ongoing Research (2025 – Present)

- Developing an inference-time, training-free defense for VLMs (e.g., CLIP/LLaVA/Flamingo) that uses **visual backtranslation** to create semantically preserving image variants and measures **joint latent-space drift**—with **patch-level alignment** of image regions to caption spans—to flag and mitigate adversarial inputs; evaluated on captioning/VQA with pixel- and latent-space attacks (FGSM, C&W, VEAttack), reporting ASR↓, clean/robust accuracy, AUROC, and latency.

## PROJECTS

### FluentAI

**An AI-powered Immersive Language Learning Platform**

Link

- Built a full-stack language tutor (Next.js + Spring Boot) with GPT-based reading, writing, speaking, and listening.

- Added handwriting/speech support and accessibility features (sign-language, Vision Pal) for inclusive learning.

### CineConnect
**A Comprehensive Web Platform for Cinema Enthusiasts**

Link

- Developed a social movie hub (Next.js, Express, Supabase) with profiles, reviews, and forums.
- Integrated theaters via Google Maps + real-time messaging/notifications to boost engagement.

### Vaxhub
**Online Vaccination System (BUET CSE FEST — DevOps Hackathon 2023)**

Link

- Implemented CI/CD with GitHub Actions; containerized and orchestrated with Docker + Kubernetes.
- Added observability and testing (Prometheus/Grafana, Jest/Supertest) for reliable deployments.

## AWARDS

- **1st Runners Up Team** in the **IEEE Signal Processing Cup 2025**, presented at **ICASSP 2025**.
- **Recipient of the Fall 2024 Richard E. Merwin Scholarship** from **IEEE Computer Society**, awarded for exceptional academic and professional potential as a **Student Ambassador**.
- **Silver Award (Runners Up)** at **Blockchain Olympiad Bangladesh 2024**, selected for the **international** round in the Netherlands.
- Received **Dean's List Award** in three out of four levels.
- **Top 10 Finalist** at Therap Javafest 2024 among 180+ teams.
- **Champion (DevOps Category)** - National Hackathon, BUET CSE FEST 2023.
- **Won 60% scholarship** at the **PTAK Case Competition 2021**.

## TECHNICAL SKILLS

- **Programming Languages:** C/C++, Java, Python, Javascript, Typescript, x86 Assembly, SQL, Bash
- **Tools & Softwares:** Git, Docker, Github Projects & Actions, Postman, DigitalOcean, Azure
- **Frameworks & Libraries:** Nodejs, Express, Spring Boot, React, Nextjs, Material UI, PyTorch, Tensorflow, Sklearn, Pandas, Matplotlib, Grafana, Prometheus
- **Database:** Oracle, PostgreSQL, Supabase

## LEADERSHIP ACTIVITIES

### IEEE Computer Society BUET Student Branch Chapter
**Vice Chairperson - Strategy**

2024 – 2025

- Led initiatives to organize technical workshops, hackathons, and industry-academia networking events to promote technical excellence among students.

### BUET Debating Club
**Director**

2024 – 2025

- Managed and organized national and international debate tournaments, fostering a culture of critical thinking and public speaking excellence within the university.

## REFERENCES

- **Dr. Md. Shohrab Hossain**, Professor
  Department of CSE, BUET
  Email: mshohrabhossain@cse.buet.ac.bd
- **Dr. Mohammad Saifur Rahman**, Professor
  Department of CSE, BUET
  Email: saifur80@gmail.com