

Shahriar Rifat

APPLIED MACHINE LEARNING RESEARCH · ROBUST AND ADAPTIVE PERCEPTION · EDGE DEPLOYMENT

rifat.s@northeastern.edu · +1 (207) 331 1980 · Boston, MA · shahriar-rifat.github.io · Scholar · GitHub · LinkedIn

SUMMARY

Machine learning researcher (Ph.D. candidate, expected April 2027) working on keeping deep models accurate after deployment, under distribution shift and adversarial attack, and cheap enough to adapt on edge hardware. Delivered in two collaborative, milestone-driven programs: a one-year industry partnership with the Technology Innovation Institute (Abu Dhabi), deploying semantic segmentation models on drone platforms, and SpectraNet, building the real-time inference engine for a deployed sensing system. 11 peer-reviewed publications (ICLR, WACV, ECCV, SPIE, IEEE TAI) and 1 U.S. patent allowed for issuance in 2026.

EDUCATION

Northeastern University

Ph.D. in Electrical Engineering, Machine Learning

June 2022 to Present

Boston, USA

Bangladesh University of Engineering and Technology

B.Sc. in Electrical and Electronic Engineering

June 2014 to October 2018

Dhaka, Bangladesh

TECHNICAL SKILLS

Machine Learning: Deep learning, computer vision, vision-language model (VLM) robustness and adaptation, test-time and online domain adaptation, adversarial robustness and model red-teaming, out-of-distribution detection and uncertainty, semantic segmentation

Deployment and Engineering: Real-time inference on embedded and edge platforms, efficient inference under resource constraints, model optimization and latency profiling, quantization, reproducible training and evaluation pipelines, multi-GPU cluster training

Frameworks and Tools: PyTorch, TensorRT, ONNX, OpenCV, NumPy, SciPy, scikit-learn, Docker, Git, SLURM, NVIDIA Jetson, Linux, Bash

Languages: Python, C/C++, MATLAB

EXPERIENCE

Applied Machine Learning Research Collaborator, Industry Partnership

Northeastern University with Technology Innovation Institute (TII), Abu Dhabi

September 2024 to December 2025

Boston, USA

- Beat the best published test-time adaptation method by 2.2 mIoU on the Cityscapes to ACDC benchmark, winning every condition (night, rain, fog, snow), by building SAGE, a shift-aware affinity-guided adaptation method; under review with TII co-authors.
- Held adaptation to 139 ms per frame, worst case 143 ms, on 4.33 GB of GPU memory: 3.8× faster and 3.6× lighter than the most expensive published method, at the highest accuracy of the seven compared.
- Deployed semantic segmentation models on TII drone platforms and owned the repository shared across both institutions through code review, reproducible pipelines, documentation, and milestone reports.

Applied Machine Learning Researcher, SpectraNet Project

Northeastern University, WINES LAB

May 2026 to Present

Boston, USA

- Exceeded the program KPIs of 90% recall and 0.40 F1 through model design and online adaptation, holding accuracy as operating conditions drift.
- Met a hard 1 ms inference budget by building the serving engine with TensorRT and integrating it into the project dApp inference framework.
- Improved performance on wild, out-of-spec inputs by more than 15% by designing a robust input ingestion and preprocessing stage.

Graduate Research Assistant

Institute for Intelligent Networked Systems, Northeastern University

June 2022 to Present

Boston, USA

- Recovered 21% accuracy over the unadapted baseline for 2.4 ms of added latency by designing DARDA, a real-time domain-adaptation method that lets deployed networks self-correct as input conditions shift (WACV 2025; patent allowed for issuance 2026).
- Exposed an unrecognized attack surface in label-free test-time adaptation (ICLR 2025) and broke adaptive perception and lane-centering stacks with projected-light attacks by building the red-team evaluation harnesses for DARPA, NSF, ARL, and AFRL funded programs.

SELECTED PUBLICATIONS AND PATENTS

- On the Adversarial Vulnerability of Label-Free Test-Time Adaptation. **S. Rifat**, J. Ashdown, M. J. De Lucia, A. Swami, F. Restuccia. *ICLR*, 2025.
- DARDA: Domain-Aware Real-Time Dynamic Neural Network Adaptation. **S. Rifat**, J. Ashdown, F. Restuccia. *IEEE/CVF WACV*, 2025. (U.S. Patent App. US 20250111667, allowed for issuance June 2026.)
- FIDEI: Hyperparameter-Free Out-of-Distribution Detection. A. Q. M. S. Sayyed, **S. Rifat**, N. D. Bastian, F. Restuccia. *IEEE/CVF WACV*, 2027.
- SAGE: Shift Aware Affinity Guided Test Time Adaptation for Semantic Segmentation. **S. Rifat**, L. Bellone, J. Simonjan, F. Restuccia. *Under review*, with TII, Abu Dhabi.
- Optical Adversaries: Assessing Robustness of Test-Time Adaptation Against Light-Based Adversarial Perturbation. **S. Rifat**, N. D. Bastian, F. Restuccia. *SPIE Assurance and Security for AI-enabled Systems*, 2026.
- Resilience of Entropy Model in Distributed Neural Networks. M. Zhang, M. Abdi, **S. Rifat**, F. Restuccia. *ECCV*, 2024.

11 peer-reviewed publications and 1 U.S. patent allowed for issuance, including ICLR, ECCV, WACV, IEEE Transactions on Artificial Intelligence, and IEEE Access, plus 2 papers under review. Full list: [shahriar-rifat.github.io](https://github.com/shahriar-rifat).

SERVICE AND TEACHING

Peer Review: ICLR (2024, 2025), NeurIPS (2026), AAAI (2025), WACV (2025), and five IEEE and Elsevier journals.

Lecturer: University of Information Technology and Sciences, Dhaka (*Feb 2020 to Present, on leave*). Taught undergraduate Machine Learning, Linear Algebra, and Robotics; designed assessments and mentored student projects.

Adjunct Lecturer: Sonargaon University, Dhaka (*Aug to Dec 2019*). Taught undergraduate Linear Systems and Digital Signal Processing.