

MD JAHIRUL ISLAM

Atlanta, GA | (404) ***-**-52 | jahirul.amsa@gmail.com | linkedin.com/in/jahirul92 | Portfolio

SUMMARY

ML researcher and engineer with 3+ years building, training, and deploying deep learning systems for computer vision, time-series sensing, and adversarial ML. Ph.D. student in AI security (4.00 GPA); first-author papers at IEEE TPS and IEEE VR; shipped production CV models in industry (YOLO, Docker, GCP, CI/CD).

EDUCATION

Kennesaw State University, *Ph.D. in Computer Science*, GPA 4.00/4.00

Jan 2025 – Present

- Research: AI security — backdoor, poisoning, and adversarial attacks/defenses for vision and language models.

Kennesaw State University, *M.S. in Computer Science (AI Concentration)*, GPA 4.00/4.00

Aug 2023 – Dec 2024

Chittagong University of Engineering & Technology, *B.Sc. in Computer Science and Engineering*

Aug 2021

TECHNICAL SKILLS

Languages: Python, C/C++, C#, Java, CUDA, SQL, Embedded C, Bash

ML / CV: PyTorch, TensorFlow, Keras, scikit-learn, OpenCV, CNNs, RNN/LSTM/GRU, GANs, Diffusion Models, LLMs & VLMs, YOLO (v6/v8/X), RTMDet, DINO, SAM, PatchCore, PaDiM, U-Net (3D), Transfer Learning, Adversarial Attacks & Defenses

MLOps & Tools: Docker, Flask, REST APIs, GitHub Actions, GCP, AWS, Git, Linux, HPC (NVIDIA A100/DGX), on-device inference (Meta Quest 3), NumPy, pandas, SQL/Firebase, Unity, Blender, Arduino/ESP32

EXPERIENCE

Kennesaw State University — ASTAI Lab

Jan 2025 – Present

Graduate Research Assistant (AI Security & Adversarial ML)

Kennesaw, GA

- Designed a robust, physically realizable backdoor attack on remote-sensing deep learning models (first author, **IEEE TPS 2025**).
- Developing clean-label backdoor/poisoning attacks and adversarial-patch pipelines in PyTorch; built a reproducible evaluation harness (attack success rate, clean accuracy) on CIFAR-10, Tiny-ImageNet, NWPU-RESISC45, and AID with ResNet.
- Co-developed **SpectraDiff**, a spectral + diffusion-model defense that detects and purifies adversarial patches (under review, AAI 2027); benchmarked defenses for remote-sensing models (**IEEE ICMLA 2025**).

Kennesaw State University — HIX Lab

Aug 2023 – Dec 2024

Graduate Research Assistant (VR / Physiological Time-Series ML)

Kennesaw, GA

- Built cybersickness-prediction models from multimodal physiological and head/eye-tracking time series using RNN, GRU, LSTM, CNN-LSTM, ResNet, and N-HiTS. [\[Code\]](#)
- Optimized and deployed models on the standalone Meta Quest 3 (Snapdragon) with Unity for real-time on-device inference; published at **IEEE VR 2024** and **IEEE VR 2025**.
- Designed a real-time, feedback-driven cybersickness detection and mitigation framework (M.S. thesis) using HP Reverb G2 Omnicept, EmotiBit, and ESP32 sensor streams.

AI Samurai Japan

Jan 2023 – Jul 2023

Machine Learning Engineer (Computer Vision)

- Developed and productionized a car image segmentation model (YOLOv6) served via a Flask REST API in Docker on GCP with GitHub Actions CI/CD.
- Built an anomaly-detection pipeline for potato quality classification (PatchCore, PaDiM, DINO, SAM); fine-tuned and benchmarked YOLOv8, YOLOX, and RTMDet on multiple datasets.
- Implemented SMPL body-model functionality and 3D/depth-map generation pipelines in Blender.

SELECTED PUBLICATIONS

full list on Google Scholar

1. **M. J. Islam**, K. A. Islam. “Robust Physically Realizable Backdoor Attack.” *IEEE TPS*, 2025. [\[Paper\]](#)
2. H. Perry, **M. J. Islam**, K. A. Islam. “SpectraDiff: Adversarial Patch Identification and Purification through Spectral and Diffusion Models.” Under review, AAI, 2027.
3. S. Ravikumar, **M. J. Islam**. “Comparative Analysis of Defense Approaches against Adversarial Attacks on Remote Sensing Applications.” *IEEE ICMLA*, 2025. [\[Paper\]](#)
4. **M. J. Islam**, R. Islam. “Towards Optimized Cybersickness Prediction for Computationally Constrained Standalone VR Devices.” *IEEE VR*, 2024. [\[Paper\]](#)

SELECTED PROJECTS

Brain Tumor Segmentation — Custom 3D U-Net for volumetric MRI tumor segmentation on the BraTS dataset. [\[GitHub\]](#)

2024

MediBox+ Smart Medicine Dispenser — ESP32/Arduino dispenser with Android reminder app (ICSADL 2026). [\[GitHub\]](#)

2023

AWARDS & SERVICE

IEEE Student Travel Grant (2025); KSU CCSE and Graduate College Research Travel Awards (2024, 2025). Reviewer, IEEE Internet of Things Journal (2025) and IEEE ICEFronT (2026); Student Volunteer, IEEE TPS 2025; IEEE Graduate Student Member.