

Abdullah Arafat Miah

+1 401-432-4536 | abdullaharafat.miah@uri.edu | [GitHub](#) | [Google Scholar](#) | Kingston, RI, USA

EDUCATION

University of Rhode Island

Ph.D., Electrical Engineering — AI/ML Security | GPA: 3.95/4.00

Kingston, RI

09/2023 – 05/2028 (Expected)

EXPERIENCE

Graduate Research Assistant, University of Rhode Island

RI, USA

Advisor: Dr. Yu Bi

Sep 2023 – Present

- Design and evaluate backdoor attacks and defenses across CNNs, Spiking Neural Networks (SNNs), and Vision-Language Models (VLMs / retrieval-augmented VLRAG pipelines).
- Built a multimodal retrieval-augmented generation pipeline (SigLIP / CLIP retriever, FAISS vector index, LLaVA generator) in PyTorch and studied its robustness at million-scale image databases.
- Developed a pruning-based backdoor mitigation method using adversarial-proxy based neuron ranking, published in *Neurocomputing* (2026).
- Built black-box and architectural backdoor defenses for deep neural networks and large language models, validated across multiple public benchmarks.

Graduate Teaching Assistant, University of Rhode Island

RI, USA

Dept. of Electrical, Computer & Biomedical Engineering

Sep 2024 – Present

- Lead undergraduate lab sections for Digital Circuit Design (ELE 202) and Digital Circuit Design with FPGAs (ELE 302) — lab prep, instruction, grading, and exam proctoring.

SELECTED PUBLICATIONS

First author on all works listed below. | 9 total publications. Full list on [Google Scholar](#). | **Service:** Reviewer, *IJCNN* 2026.

- “Multi-Knowledge Poisoning Attack with Backdoored Retriever on RAG-based Vision-Language Models.” *In preparation* — targeting *NAACL 2027* (ARR Oct. 2026 cycle).
- “DeepCurer: Pruning-based Backdoor Mitigation via Progressive Neuron Ranking using Adversarial Proxies.” *Neurocomputing*, 2026, art. 134409.
- “Lite-BD: A Lightweight Black-box Backdoor Defense via Reviving Multi-Stage Image Transformations.” *IEEE/INNS IJCNN* 2026 (Accepted).
- “T-Backdoor: Exploiting Temporal Redundancy in Neuromorphic Data for Spike-preserving Backdoor Attacks on SNNs.” *IEEE Transactions on Artificial Intelligence* (Under Review).
- “NoiseAttack: An Evasive Sample-Specific Multi-Targeted Backdoor Attack Through White Gaussian Noise.” *International Journal of Information Technology* (Accepted).
- “BadSNN: Backdoor Attacks on Spiking Neural Networks via Adversarial Spiking Neuron.” *Neurocomputing* (Under Review).
- “Exploiting the Vulnerability of Large Language Models via Defense-Aware Architectural Backdoor.” *SN Computer Science* (Under Review).

SELECTED PROJECTS

Perplexity-Based Defense Against LLM Backdoor Attacks | [GitHub](#)

- Implemented a word-trigger LLM backdoor and a perplexity-based defense; showed defense efficacy degrades sharply as trigger length grows.

Sentiment & Emotion Recognition via Attention-based LSTM | [GitHub](#)

- Built an LSTM with an added attention layer for joint sentiment and emotion classification from text.

Real-Time Drowsiness Detection using CNN + Eye Landmarks | [GitHub](#)

- Fused eye-landmark distance features with a custom CNN for real-time video-based drowsiness detection; published (Springer AISC).

SKILLS

- Languages:** Python, C++, C, R, Julia
- ML/DL Frameworks & Tools:** PyTorch, TensorFlow, Keras, Scikit-Learn, OpenCV, Pandas, NumPy, FAISS, Git, Linux, MATLAB
- Focus Areas:** Machine Learning, Deep Learning, Computer Vision, Multimodal/Vision-Language Models, Adversarial ML and Model Security