Tahmid Hasan Pranto

305 S Gay St Apt 109, Auburn, AL 36830, USA.

Profiles & Contact: Google Scholar | (+1) 5412507859 | tahmidpranto1406@gmail.com | Personal Website | GitHub | Researchgate | LinkedIn

Research Interest

My research interests lie broadly in Machine Learning, with working experience on LLM robustness, adversarial machine learning, deep learning for computer vision, and secure AI system deployment.

Education

Master of Science (M.Sc.) in Computer Science

Sep 2023 - Mar 2025.

Oregon State University | Cum Laude | CGPA: 3.57/4 *Corvallis, OR 97333, USA*

Project Title: Hessian-aware Training for Enhancing DNNs Resilience to Parameter Corruptions

Bachelor of Science (B.Sc.) in Computer Science and Engineering

April 2021

North South University | Cum Laude | CGPA: 3.57/4 *Dhaka 1229, Bangladesh*

Thesis: Effect of label noise in semantic segmentation of sedimentation from high-resolution satellite imagery.

Work Experience

Graduate Research & Teaching Assistant

Sep 2023 - Mar 2025

Electrical Engineering and Computer Science at Oregon State University

Major Responsibilities:

- Conducting comprehensive reviews of scientific literature aligning with the research objectives.
- Designing, implementing, and executing experiments on specified datasets and DNN/LLM models to identify and analyze security vulnerabilities.
- Engineering defense mechanisms to effectively mitigate identified vulnerabilities.
- Creating visualizations to illustrate findings; writing comprehensive reports to document the experimental process and outcomes aiming to be published in scientific conferences and journals.
- As GTA for CS374 (Operating Systems), attended weekly office hours to assist students with course materials and graded assignments and exams.

Senior Research Assistant

May 2021 - Aug. 2023

Electrical & Computer Engineering at North South University

Major Responsibilities:

- Developing novel hybridization techniques of distributed platforms (such as e-commerce) using Blockchain and Machine Learning.
- Reviewing scientific research papers, designing and conducting experiments, and analyzing results.
- Writing academic papers which have been published in academic journals and conferences.
- Supervising senior year undergrad students in their thesis and collaborating with undergraduate research assistants.

Academic Research & Projects

Hessian-aware Training for Enhancing DNN Resilience to Parameter Corruptions

Master's Project Funded by Samsung Global Research Outreach (GRO)) *Aug 2023 - Mar 2025*

- Proposed a Hessian-aware training algorithm that minimizes the Hessian trace to promote flatter loss surfaces, enhancing DNN resilience against parameter corruptions and bit-flip attacks.
- Conducted experiments on MNIST, CIFAR-10, and ImageNet with CNNs, ResNets, and Vision Transformers, achieving a 6–12% reduction in vulnerable parameters without sacrificing accuracy.
- Demonstrated that models trained with this method require 3× more bit-flips to induce severe accuracy drops compared to baseline models.
- Showed compatibility with hardware/system-level defenses (e.g., NeuroPot, RADAR), reducing runtime and storage overheads while strengthening robustness.

End-to-End LLM Chatbot

Personal Project *Apr 2025*

- Connected the LLaMA2 model and a Retrieval-Augmented Generation (RAG) pipeline for context-aware responses.
- Built document ingestion, embeddings (ChromaDB), and vector search for retrieval.
- Built full-stack LLM chatbot with a FastAPI backend and React frontend.

Fully Supervised Action Segmentation

AI637-Computer Vision II (Course Project) *Aug 2023 - Mar 2025*

- Implemented a Vision Transformer (ViT)-based end-to-end action segmentation model with VideoMAEv2 backbone.
- Achieved 97.4 F1@10 on the GTEA dataset, outperforming state-of-the-art baselines (MSTCN, ASFormer, DiffAct, FACT).
- Evaluated frozen vs adapter fine-tuning and downsampling strategies, demonstrating high accuracy across multiple benchmarks (GTEA, 50Salads, Breakfast).

Semantic Segmentation of Sedimentation using DNNs

Bachelor's Thesis. Funded by Faculty Research Grant - CTRG-21-SEPS-19) *Apr 2021*

- Constructed a high-resolution dataset of the Bangladesh marine region using Copernicus Sentinel-2 imagery, labeled into five sedimentation classes using ARCGIS/QGIS.
- Designed and implemented a modified U-Net architecture with patch-wise learning, enabling efficient training on extremely large satellite image tiles (36k × 28k pixels).
- Achieved strong performance with Dice Coefficient up to 87% and pixel accuracy 77%, demonstrating the effectiveness of deep learning for large-scale marine sediment analysis.
- Extended the study by investigating the impact of label noise (NCAR, NAR, NNAR) on semantic segmentation, providing systematic evaluations of robustness to noisy labels in satellite-based environmental monitoring.

Selected Publication

- (Sumbitted to Transactions on Machine Learning Research - TMLR) **Tahmid Hasan Pranto,** Seijoon Kim, Lizhong Chen, Sanghyun Hong (2025), Hessian-aware Training for Enhancing DNN Resilience to Bitwise Corruptions in Their Parameters.
- **Tahmid Hasan Pranto,** Noman A.A., Noor A., Deepty U.H., Rahman R.M. (2022) **Effect of Label Noise on Multi-Class Semantic Segmentation : A Case Study on Bangladesh Marine Region,** Applied Artificial Intelligence, Springer.
- **Tahmid Hasan Pranto,** Noman A.A., Noor A., Deepty U.H., Rahman R.M. (2021), **Patch-Wise Semantic Segmentation of Sedimentation from High-Resolution Satellite Images Using Deep Learning.** Advances in Computational Intelligence, IWANN 2021. Lecture Notes in Computer Science, vol 12861. Springer, Cham.
- **Tahmid Hasan Pranto,** Neloy M.N., Noman A.A., Wasif S., Wahab M.A., Rahman M.R., 03 January 2024, **Utilizing deep learning in chipless RFID tag detection: an investigation on high-precision mm-wave spatial tag estimation from 2D virtual imaging,** Journal of Information and Telecommunication.
- Noman, A. A., Akter, U. H., **Tahmid Hasan Pranto**, & Haque, A. K. M., **Machine Learning and Artificial Intelligence in Circular Economy: A Bibliometric Analysis and Systematic Literature Review, 6.2 (2022): 13-40,** Annals of Emerging Technologies in Computing (AETiC).
- Noman, A. A., Rahman M., **Tahmid Hasan Pranto,** Rahman R. M., 2023,**Blockchain for Medical Collaboration: A Federated Learning-Based Approach for Multi-class Respiratory Disease Classification.,** Healthcare Analytics(Elsevier)
- Mahmud M. A. I., Talukder A. T., Sultana A., Bhuiyan K. I. A., Rahman M. S., **Tahmid Hasan Pranto,** Rahman M., 2023, **Toward News Authenticity: Synthesizing Natural Language Processing and Human Expert Opinion to Evaluate News,** IEEE Access.

Key Skills

Language & Tools	- Python, C/C++, Java, SQL, LaTeX, Git, Linux, HPC
ML/DL Frameworks	- PyTorch, TensorFlow, Scikit-Learn, OpenCV, Hugging Face, Transformers, LangChain
Generative AI & LLMs	- Hugging Face, LangChain, RAG, ChromaDB, Transformers
Data Science & Analysis	- Pandas, NumPy, Matplotlib, Seaborn, SciPy
Web & Cloud	- React.js, FastAPI, Django, REST APIs, Docker
Soft Skills	- Research writing, Collaboration, Communication, Teamwork

Certifications

- Machine Learning — Coursera | Stanford University (Andrew NG) — Jul 2021
- AWS Certified Cloud Practitioner — AWS — Jul 2025
- LangChain for LLM Application Development — DeepLearning.AI — Aug 2025
- Generative AI with Diffusion Models — DeepLearning.AI — Aug 2025
- Deep Learning Specialization (5 Courses) — Coursera | DeepLearning.AI — Jun 2021 – Oct 2021
  - Neural Networks and Deep Learning
  - Improving Deep Neural Networks: Hyperparameter Tuning, Regularization and Optimization
  - Structuring Machine Learning Projects
  - Convolutional Neural Networks

Extracurricular Activities

- General Member, Association for the Advancement of Artificial Intelligence (AAAI) — Apr 2024 - Present
- Advisor, Shabash Fakibaj LLC — 2022 – Present
  - A volunteer initiative supporting undergraduates in navigating higher study opportunities overseas.

References

Available upon request.