Hasanul Mahmud, Ph.D.

7550 Country Club Drive Apt 12201, Laredo, TX 78041
Email: hasanulislam2599@gmail.com — Phone: +1-210-723-0234
LinkedIn: linkedin.com/in/hasanul-islam
GitHub: github.com/max2022

Professional Summary

I am a research-focused computer scientist with extensive doctoral and postdoctoral experience in developing energy-efficient, low-latency deep learning models for deployment on edge devices and cloud platforms. My Ph.D. research focused on designing robust deep neural network (DNN) architectures capable of resisting adversarial threats, including white-box and black-box attacks, using TensorFlow, PyTorch, and embedded AI tools. As a postdoctoral researcher, I expanded my expertise to the security of large language models (LLMs), analyzing their vulnerabilities and exploring mitigation strategies against adversarial, backdoor, and data poisoning attacks. Complementing my research, I have over five years of teaching and mentoring experience at both undergraduate and graduate levels, including course instruction, curriculum design, and the development of practical, hands-on assignments for in-person and online learning. I am passionate about building secure, trustworthy AI systems while fostering inclusive and engaging educational environments.

Education

- **PhD in Computer Science**, University of Texas at San Antonio, 2019–2025
- **M.Sc in Computer Science**, University of Texas at San Antonio, 2019–2023
- **B.Sc in Computer Science**, University of Dhaka, 2012–2017

Work Experience

Visiting Assistant Professor, Texas A&M International University   August 2025–Present

- Instructing undergraduate courses in Computer Science and Engineering, including:
  - CSCE 1337: Object-Oriented Programming
  - CSCE 4300: Digital Electronic Circuit Design
  - ENGR 2105: Principles of Electrical Engineering Lab
  - CSCE 1136: Fundamentals of Programming Lab
- Preparing lab materials, programming assignments, and hands-on exercises to enhance student engagement and practical skills.
- Providing academic guidance and support to students through office hours, lab assistance, and project mentoring.
- Collaborating with faculty to align course content with program objectives.

Postdoctoral Research Fellow, University of Texas at San Antonio.   June 2025 – August 2025

- Designing task-oriented conversational agents to assist cancer patients with appointment scheduling, medication adherence, and symptom tracking.

- Evaluating dialogue system performance across NLU, policy management, and response generation for healthcare-specific intents.

- leading a study on assessing chatbot systems in clinical communication scenarios with a focus on safety, interpretability, and patient experience.

- Collaborating with interdisciplinary teams across AI, healthcare, and human-computer interaction for scalable deployment of secure NLP systems.

Graduate Research Assistant, University of Texas at San Antonio   Jun 2020 – May, 2025

- Conducted research on energy-efficient, low-latency deep learning frameworks for deployment on edge devices such as Raspberry Pi and Jetson Nano.

- Designed robust DNN architectures and defense strategies against adversarial attacks (e.g., FGSM, PGD, backdoor), contributing to multiple first-author publications in top-tier conferences (IPDPS, IEEE Cloud, ICPR).

- Proposed and implemented converting autoencoder-based architectures to improve DNN classification accuracy under SLO and energy constraints.

- Led benchmarking and profiling of inference latency, energy usage, and throughput of deep learning models across embedded and cloud platforms.

- Mentored undergraduate and MS students in research methodology, experimental setup, and model evaluation; provided feedback on their theses and paper drafts.

- Supported lab operations by configuring hardware/software stacks, documenting reproducible workflows, and assisting in preparing grant proposals (e.g., NSF submissions).

Graduate Teaching Assistant, University of Texas at San Antonio   Aug 2019 – May,2025

- Assisted and independently led lectures, labs, and assignments for undergraduate and graduate computer science courses.

- Created and graded assignments, projects, and exams; managed in-person and online students.

- Contributed to syllabus and curriculum design for core systems and AI-related courses.

- Mentored students in algorithm design, programming, and high-performance computing frameworks.

- **Courses Assisted:**
  - Spring 2025 – High-Performance Machine Learning, Analysis of Algorithms
  - Fall 2024 – Parallel Computing
  - Spring 2024 – Parallel Algorithms
  - Spring 2023 – High-Performance Computing
  - Fall 2022 – Parallel Computing
  - Spring 2022 – High-Performance Computing
  - Summer 2022 – Cloud Computing
  - Summer 2021 – Application Programming
  - Spring 2021 – High-Performance Computing
  - Summer 2020, Spring 2020 – Discrete Mathematics

    – Fall 2019 – Computer Programming

Software Engineer, Placovu Inc., Dhaka, Bangladesh   2017 – 2018

- Built backend systems using Java and C#.

- Optimized search performance using Elasticsearch and SQL Server.

Technical Skills

Languages: Python, Java, C++, R, SQL, Rust
Frameworks & Tools: TensorFlow, PyTorch, Keras, Docker, Git, OpenMP, MPI, CUDA, PySpark, Hadoop
Visualization: Tableau, Power BI, Seaborn, Matplotlib
Hardware/Testbeds: Raspberry Pi 4, Jetson Nano, Chameleon Cloud, DGX Cluster, Stampede

Publications

- *A Converting Autoencoder Toward Low-latency and Energy-efficient DNN Inference at the Edge*, IPDPS 2024

- *CAE-Net: Enhanced Converting Autoencoder based Framework for Low-latency Energy-efficient DNN with SLO-constraints*, IEEE Cloud Summit 2024

- *EncodeNet: A Framework for Boosting DNN Accuracy with Entropy-driven Generalized Converting Autoencoder*, ICPR 2024

Work in Progress

- **Efficient Detection of Backdoor Attacks** – Designed a framework to detect backdoor attacks by perturbing inputs and analyzing model activations and entropy.

- **Energy Consumption Benchmarking of Individual Layers in Deep Neural Networks** – Conducted detailed experiments to measure energy usage, memory consumption, CPU utilization, and latency of each layer in various DNNs on Raspberry Pi and Jetson Nano.

- **Vulnerability Analysis in Deep Neural Networks** – Evaluated widely-used DNN models under both white-box and black-box attacks. Analyzed activation patterns, entropy, and saliency maps using Explainable AI techniques to identify vulnerabilities across layers.

Research Projects

- **Modular Autoencoders for Improving DNN Classification Accuracy** – Explored clustering methods to capture intra- and inter-class relationships for hierarchical DNN design. Proposed modular architectures to reduce the memory footprint.

- **Designing Memory-Aware Frameworks for Tiny Edge Devices** – Developed multiple lightweight DNN models with fewer than 20K parameters and <84KB size, achieving over 80% accuracy on CIFAR-10, enabling deployment on highly constrained devices.

Academic Projects

- **Adversarial Vulnerability Analysis of Deep Neural Networks** – Studied attacks (PGD, FGSM, CW, Trojan) on VGG, ResNet, ShuffleNet. Tools: PyTorch, TensorFlow, Jetson Nano, Raspberry Pi.

- **Energy-Aware DNN Benchmarking on Edge Devices** – Layer-wise energy measurement; proposed energy-aware pruning.

- **Distributed Healthcare System via Java RMI** – Built secure backend system for distributed healthcare data.

- **Operating System Caching Mechanism** – Simulated caching to evaluate page hits/misses.

- **Animated Road Traffic Simulation** – Real-time simulation of cars/pedestrians.

- **E-Commerce Shopping Platform** – Online shop with full cart/order/user interface.

- **Fruit Ninja Game** – Built an OpenGL/OpenCV fruit slicing game.

- **Library Management System** – Book tracking system with user/librarian interface.

- **Line-Following Robot with Bluetooth Control** – Robot navigation and manual override via Bluetooth.

- **Police Department Database System** – Centralized personnel tracking system with web UI.

Conferences & Workshops

- IEEE Cloud Summit 2024 (Presenter)

- IPDPS PhD Forum 2022 (Presenter)

- UTSA Graduate Research Symposium 2022 (Presenter)

- MVAPICH User Group Conference, 2022 at Ohio State University (Presenter)

- NSF AI Spring School, 2024 at UTSA (Presenter)

Honors & Awards

- NSF Travel Grant — MUG 2022

- TCPP Award to Attend – IPDPS 2024

- Finalist — Radiance Innovation Bowl 2023

- UTSA Graduate School Professional Development Award 2024

Certifications

- HackerRank: Problem Solving (Intermediate)

- Solved 350+ Algorithmic Problems on LeetCode.

References

Available upon request.