Maisha Binte Rashid

Waco, Tx maishabrashid05@gmail.com 254-224-2825 Maisha Binte Rashid maisha05

Career Profile

Specializing in multimodal machine learning and AI robustness, with expertise in integrating text and image data to defend against adversarial attacks. Proficient in Python, PyTorch, and TensorFlow, with experience in large-scale language models (LLMs), NLP, and deep learning. Proven track record of contributing to NSF-funded projects and publishing in AI conferences. Actively seeking opportunities to apply my skills in AI research and development to solve complex, real-world challenges.

Education

Baylor University *Aug 2021 – May 2026*
Ph.D. in Computer Science

- **Coursework:** Software Engineering, Advanced Database, Machine Learning, Advanced Algorithm

Ahsanullah University of Science and Technology *Jun 2015 – Jun 2019*
B.Sc. in Computer Science

- **Coursework:** Structured Programming, OOP, Data Structures, Algorithms, Database Management, Software Engineering

Skills

- **Programming Languages:** C# (Advanced), C++ (Good), Python (Advanced), JAVA (Fair), TypeScript (Advanced)
- **Messaging and Event Streaming:** Apache Kafka, RabbitMQ
- **Frameworks and Libraries:** TensorFlow (Advanced), PyTorch (Advanced), Scikit-learn (Advanced), Transformers (Advanced), JAX (Good), CUDA (Good)
- **Databases:** MongoDB, Oracle, SQL, MySQL
- **Tools:** VS Code, Jupyter, UNIX, Pycharm, Git, HuggingFace

Experience

Graduate Assistant *Waco, Tx*
Baylor University *Aug 2021 –Present*

- Enhanced **AI safety** for models like **GPT-2** and **Vision Transformer**, defending against adversarial attacks. Integrated image and text data, boosting accuracy by 12%.
- As a research assistant, contributed as a lead in a multimodal deep learning project, focusing on image and text data analysis. Played a pivotal role in an NSF-funded project, using **Flamingo** to accurately identify stolen car parts from a comprehensive 400 GB dataset of Craigslist images and posts, showcasing exceptional data analysis and machine learning capabilities.
- Spearheaded Developed a risk assessment metric for vision–language models, the **Adversarial Vulnerability Index (AVI)**, by running a progressive stress test **(random noise to gradient-based attacks)** and quantifying vulnerability as the normalized differential performance drop between stochastic noise and adversarial perturbations.
- Directed student engagement in a graduate Natural Language Processing (NLP) course, advancing competencies in machine learning models and text analysis.

Programmer Analyst *Dhaka, Bangladesh*
Computer Ease Ltd. *Jan 2020 – Jul 2021*

- Led development of 20 modules across 4 websites for B2B transactions, using **.NET** and **C#**. Reduced processing time by 30%, enhancing client operations.
- Developed two client dashboards for daily transaction monitoring using **Angular** and **.Net Core**. Dropped error rates by 40%, improving data fidelity.

Publications

- **M. Rashid**, P. Rivas, “AI Safety in Practice: Enhancing Adversarial Robustness in Multimodal Image Captioning”, Ethical AI Workshop at ACM KDD’24.
- **M. Rashid**, MS Rahaman, P. Rivas, “Navigating the Multimodal Landscape: A Review on Integration of Text and Image Data in Machine Learning Architectures” at Machine Learning and Knowledge Extraction Journal
- **M. Rashid**, P. Rivas, “Scoping Review on Image-Text Multimodal Machine Learning Models” at 2023 International Conference on Computational Science and Computational Intelligence
- O. Hoque, **M. Rashid**, T. Zawad, “Autonomous deblurring images and information extraction from documents using CycleGAN and mask RCNN” at 23rd International Conference on Computer and Information Technology (ICCIT)

  M. Rashid, T. Zawad, S. Nazmus, “Targeted face recognition and alarm generation for security surveillance using single shot multibox detector (SSD)” at International Journal of Computer Applications

Projects

Adversarial Robustness increase in Vision Language models *Project Link*

- Develop multimodal machine learning model to perform image captioning task using **ViT** and **GPT-2**.
- Alternatively freeze ViT and GPT-2 to find vulnerable modality and perform adversarial training to the model to find efficient way to increase robustness. By finding the weaker modality and freezing the less vulnerable modality increased model performance from 74% to 78%.

Analyzing-Adversarial-Vulnerability-of-Stable-Diffusion *Project Link*

- Fine-tuned Stable Diffusion on the COCO dataset for text-to-image generation.
  Applied gradient-based attacks (FGSM, PGD) to the image latent component and text-based attacks (TextAttack, prompt perturbations) to the prompt component.
  Measured robustness using LPIPS (perceptual change) and CLIP score (image-text alignment) to quantify degradation under attack.

Adversarial Sensitivity analysis metric for VLMs *Project Link*

- Ran a controlled modality stress test on **CLIP** by alternately freezing the **ViT (vision) and text encoders** and attacking with gradient-based methods on Hateful Memes; the vision modality showed a 9% larger accuracy drop than the text modality.
- Defined the Adversarial Vulnerability Index (AVI), a progressive evaluation from random noise to gradient-based attacks, quantifying risk as the normalized differential performance drop between stochastic noise and **adversarial perturbations**.

Cyberbullying detection using SVM and KNN *Project Link*

- Applied three machine learning supervisor and unsupervised algorithms - **Logistic Regression**, **SVM**, and **KNN** - for detecting cyberbullying in social media posts.
- Conducted comprehensive analysis using these algorithms to identify and classify abusive language effectively in various social media content.

CyberPolice *Project Link*

- Developed three deep learning models - **LSTM**, **Bi-LSTM**, and **Bi-LSTM** with Transformer - for cyberbullying detection in Facebook post datasets.
- Employed these models for sentiment analysis in social media content, accurately identifying the emotional context of posts.
- Enhanced cyberbullying detection precision through innovative application of natural language processing and deep learning techniques