

MOHD. FARHAN ISRAK SOUMIK

+1(781)698-8513 ◇ Carbondale, Illinois, USA

Email ◇ Website ◇ Google Scholar ◇ ORCID ◇ ResearchGate ◇ GitHub ◇ LinkedIn

RESEARCH INTERESTS

My research examines the security, privacy, and forensic challenges of human interaction with large-scale, consumer-facing generative AI systems, with an emphasis on building trustworthy and human-centered AI. I study privacy risks arising from implicit behavioral signals, defend against deceptive uses of generative AI, and explore quantum machine learning for attention mechanisms and critical infrastructure.

Technical Focus Areas: Privacy-preserving machine learning; large language models (LLMs); vision-language models (VLMs); multimodal AI; generative AI forensics; federated learning; quantum machine learning.

CAREER GOALS

- **Short-term Goal:** To complete my M.Sc. with a strong record of high-impact research in secure, privacy-preserving, and trustworthy AI, and to continue into a Ph.D. with an independent research agenda at the intersection of generative AI, multimodal learning, and human-centered security.
- **Long-term Goal:** To pursue a faculty position in computer science, where I can lead an interdisciplinary research program, mentor graduate and undergraduate students, and contribute through teaching, scholarship, and service to advancing responsible and trustworthy AI systems.

EDUCATION

Southern Illinois University Carbondale (SIUC), IL, USA 2024 – 2027 (expected)

M.Sc. in Computer Science CGPA **4.00 (on the scale of 4.00)**

Supervised by: Dr. Abdur Rahman Bin Shahid, Assistant Professor & Director of SHIELD Lab, School of Computing, SIUC.

Rajshahi University of Engineering & Technology (RUET), Bangladesh 2016 – 2020

B.Sc. in Computer Science & Engineering CGPA **3.47 (WES) (on the scale of 4.00)**

Thesis: An analysis of the impact of deep learning based models for classification and segmentation of tumors from medical images.

Supervised by: Dr. Md. Ali Hossain, Professor, Dept. of Computer Science and Engineering, RUET.

PUBLICATIONS

Conference Papers

- [C1] **M. F. I. Soumik**, A. A. Fime, W. K. M. Mithsara, A. B. Aryal, H. J. Haghighi, B. Koirala, A. Imteaj, and A. R. Shahid, “**Edits in the Wild: A Multilingual Benchmark for Localizing On-Device Generative Image Edits on Consumer Platforms**,” *Proceedings of the 2026 Conference on Empirical Methods in Natural Language Processing (EMNLP 2026), Main Conference*. [To appear]
- [C2] **M. F. I. Soumik**, S. M. Hasan, W. K. M. Mithsara, A. R. Shahid, and A. Imteaj, “**No Innocence in Styling: Discovery of Privacy Protection Capabilities and Security Risks in Consumer Generative AI Writing Assistants**,” *Proceedings of the 64th Annual Meeting of the Association for Computational Linguistics (ACL 2026), Industry Track*. [ACL Anthology]
- [C3] **M. F. I. Soumik**, H. Zangoti, A. B. Aryal, A. Imteaj, and A. R. Shahid, “**When Quantum Entanglement Meets Transformer Attention: A Controlled Study of Quantum Attention Heads**,” *Proceedings of the 38th IEEE International Conference on Tools with Artificial Intelligence (ICTAI 2026)*. [To appear]
- [C4] **M. F. I. Soumik**, E. Maghsoudlou Nima, H. Zangoti, A. Imteaj, and A. R. Shahid, “**Privacy-Preserving Multimodal Stress Detection from Wearables with Attention Fusion and Federated Learning**,” *Proceedings of the 24th IEEE International Conference on Machine Learning and Applications (ICMLA 2025)*. [IEEE Xplore]
- [C5] **M. F. I. Soumik** and M. A. Hossain, “**Brain Tumor Classification with Inception Network Based Deep Learning Model Using Transfer Learning**,” *Proceedings of the 2020 IEEE Region 10 Symposium (TENSYP 2020)*. [IEEE Xplore]

Workshop Papers

- [W1] M. F. I. Soumik, W. K. M. Mithsara, A. R. Shahid, and A. Imteaj, “**Audio Editing Features as User-Centric Privacy Defenses Against Large Language Model (LLM)-Based Emotion Inference Attacks**,” *Proceedings of the 6th AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI-25)*, co-located with AAAI 2025. [arXiv]

Journal Papers (Under Review)

- [J1] M. F. I. Soumik and A. R. Shahid, “**Before the First Circuit: Zero-Shot Quantum Kernel Screening on Foundation Models with Kernel-Target Alignment**,” *Quantum Machine Intelligence* (Springer), 2026. [Under review]
- [J2] M. F. I. Soumik, M. M. W. Kankanamge, A. B. Aryal, P. Neupane, A. Barua, M. A. Hossain, and A. R. Shahid, “**Quantum AI in Cyber-Physical Systems for Critical Infrastructure: Architectures, Applications and Future Directions**,” *Quantum Information Processing* (Springer), 2026. [Under review]

Preprints

- [P1] M. F. I. Soumik, S. M. Hasan, and A. R. Shahid, “**Evaluating Apple Intelligence’s Writing Tools for Privacy Against Large Language Model-Based Inference Attacks: Insights from Early Datasets**,” *arXiv preprint arXiv:2506.03870*, 2025. [arXiv]

RESEARCH EXPERIENCE

Graduate Research Assistant

Center for Virtual Expression ([CVEX](#)), The Arch, SIUC

August 2026 – Present

Carbondale, Illinois, USA

- Building a localized, LLM-based tutoring application for CVEX, running Gemma 4 on-device with retrieval-augmented generation (RAG) over course material, under Dr. Holly Lewis.
- Research on human–AI agent interaction and its social impact.

Graduate Research Assistant

Secure and Trustworthy Intelligent Systems Lab ([SHIELD Lab](#)), SIUC

June 2025 – July 2026

Carbondale, Illinois, USA

- Conducted research on large language models, vision-language models, and usable privacy and security under Dr. Abdur Rahman Bin Shahid.
- **Key Achievements:**
 - Built the first large-scale, multilingual benchmark of on-device generative AI image edits from consumer platforms such as Apple Intelligence and Samsung AI, for detecting and localizing edited content [C1].
 - Showed that one-tap stylization in consumer AI writing assistants protects users from emotion-profiling attacks while also letting misinformation evade detectors [C2, P1]; evaluated audio editing as a user-side defense against LLM emotion inference [W1].
 - Designed a federated, attention-fusion model for privacy-preserving stress detection from wearables [C4]; studied quantum attention heads in transformers [C3] and zero-shot quantum kernel screening on foundation models [J1].

Research Assistant

Center for Computational and Data Sciences ([CCDS](#)), Independent University, Bangladesh

January 2022 – June 2023

Dhaka, Bangladesh

- Developed data-level fusion models for LULC classification of satellite images and segmentation models for Synthetic Aperture Radar (SAR) imagery, in collaboration with the Data & Design Lab ([DND Lab](#)), University of Dhaka.

Data Science and Business Analytics Intern

The Sparks Foundation

July 2021 – August 2021

Remote (Singapore)

- Applied Random Forest, SVM, RNN, and LSTM models to business prediction problems.

TEACHING EXPERIENCE

Graduate Teaching Assistant

School of Computing, Southern Illinois University Carbondale (SIUC)

August 2024 – June 2025; August 2026 – Present

Carbondale, Illinois, USA

- Courses: CS 220B Computer Concepts and AI (Fall 2026); Design and Analysis of Algorithms, Advanced Computer Networks (Fall 2024); Advanced Operating Systems, Computer Algorithms (Spring 2025).
- Held 20 hours/week of office hours; prepared quizzes and assignments and graded exams and coursework.

GRE Instructor

Graduate Resources Enhancing Center (GREC)

July 2023 – July 2024

Dhaka, Bangladesh

- Taught Quantitative, Verbal, and Analytical Writing; designed quizzes and graded full-length mock exams.

Teaching Assistant

Independent University, Bangladesh (IUB)

January 2022 – June 2023

Dhaka, Bangladesh

- CSC-101 Introduction to Programming, CSC-203 Data Structures, CIS-101 Fundamentals of Computer Systems; wrote a new Python lab manual when the intro course moved from C to Python.

SKILLS

Core Technical Areas	Machine Learning and Multimodal Learning; Computer Vision; Signal Processing; Security and Privacy of AI Systems; Quantum Machine Learning; Data Science
AI Skills	Generative AI; Large Language Models (LLMs); Vision–Language Models (VLMs); Agentic AI; RAG; Privacy-Preserving AI; AI Forensics; LoRA Fine-tuning; RL Post-training (GRPO)
Programming Skills	Python, MATLAB, R, Java, C, C++, Assembly
Frameworks & Libraries	TensorFlow, Keras, PyTorch, Scikit-learn, Pandas, OpenCV
Languages	Bangla (native), English (professional), German (limited), Hindi (elementary)

SERVICE & PRESENTATIONS

- **Student Volunteer**, 2026 Conference on Empirical Methods in Natural Language Processing (EMNLP 2026).
- **Student Volunteer**, 64th Annual Meeting of the Association for Computational Linguistics (ACL 2026).
- Poster, *No Innocence in Styling* [C2], ACL 2026, San Diego, CA, July 2026.
- Talk, *Privacy-Preserving Multimodal Stress Detection* [C4], ICMLA 2025, Boca Raton, FL, Nov. 2025.
- Poster, *Audio Editing Features as User-Centric Privacy Defenses* [W1], AAAI PPAI-25 Workshop, Feb. 2025.

AWARDS & ACHIEVEMENTS

- **Diversity & Inclusion Subsidy Grant(D&I)** for presenting my paper at ACL 2026.
- **Travel Grant** for Poster Presentation at the 6th AAAI Workshop on Privacy-Preserving AI (PPAI-25).
- Government Scholarship and full tuition waiver for 85th place (top 5%) in the national HSC merit list, 2015.
- Solved **500+** problems on HackerRank, LeetCode, and UVA; Gold badge on [HackerRank](#) ([LeetCode](#)).

CERTIFICATIONS

Machine Learning (Stanford University) [\[Link\]](#) ◇ *Deep Learning Specialization* (DeepLearning.AI) [\[Link\]](#) ◇ *Generative AI with LLMs* (DeepLearning.AI) [\[Link\]](#) ◇ *TensorFlow Developer Professional Certificate* (DeepLearning.AI) [\[Link\]](#) ◇ *Mathematics for Machine Learning* (Imperial College London) [\[Link\]](#)

TEST SCORES

GRE: 317 (Quant 164, Verbal 153, AWA 4.0) ◇ **IELTS:** 8.0 (L 8.5, R 8.5, W 7.0, S 7.0)

REFERENCES

Dr. Abdur Rahman Bin Shahid Assistant Professor, School of Computing, Southern Illinois University Carbondale (SIUC). Email: shahid@cs.siu.edu	Dr. Ahmed Imteaj Assistant Professor, Dept. of Electrical Engineering and Computer Science, Florida Atlantic University. Email: aimteaj@fau.edu
---	--