

Mushtari Sadia

PhD Candidate @ UMich-Ann Arbor

Research Areas: AI Agent Systems, LLMs, Multi-Modal AI, Security & Privacy

Location: Ann Arbor, MI, USA

Email: mushtari@umich.edu

Mobile: +17346578720

[Website](#) | [LinkedIn](#) | [Scholar](#)

Education

University of Michigan – Ann Arbor	2024 - Present
Ph.D. in Computer Science and Engineering	
Advisors: Prof. Ang Chen and Prof. Amrita Roy Chowdhury	
University of Michigan – Ann Arbor, M.Sc. in Computer Science and Engineering	2026
Bangladesh University of Engineering and Technology, B.Sc. in CSE	2023

Work Experience

Graduate Student Research Assistant, Michigan Systems Laboratory	Aug 2024 – Present
Research in Agentic Systems, Unstructured Data, Multimodal Reasoning, and Privacy Preserving Computation . Building systems that provide privacy, reliability, and integrity guarantees for LLM based computation over unstructured and multimodal data.	
Research Intern, MIT Camera Culture Group (Fatima Fellowship)	Jun 2023 - Mar 2023
Supervisor: Dr. Praneeth Vepakomma	
Research in Distributed ML, Parallelizing Neural Network Training .	
Graduate Student Instructor, University of Michigan, Ann Arbor	Jan 2026 – Apr 2026
Lecturer, CSE, BRAC University, Dhaka, Bangladesh	Jun 2023 – Aug 2024
Adjunct Lecturer, CSE, BUET, Dhaka, Bangladesh	Nov 2023 – Mar 2024

Publications

1 SQUiD: Synthesizing Relational Databases from Unstructured Text	2025
Mushtari Sadia, Zhenning Yang, Yunming Xiao, Ang Chen, Amrita Roy Chowdhury	
EMNLP 2025 (Oral Presentation, 2.75% selection rate) Paper link	
Designed a novel neurosymbolic framework that automatically <i>synthesizes relational databases from unstructured text</i> by generating its schema and populating its tables from raw text. Designed a four stage pipeline, each with specialized techniques, achieving up to 91% entity coverage with 100% primary and foreign key validity, and improving upto 18× over direct LLM prompting baselines.	

Preprints

2 Pimento: A Privacy Framework for Querying Text	2026
Mushtari Sadia, Ang Chen, Amrita Roy Chowdhury	
Under review at USENIX Security 2027 Preprint	
Developed Pimento , which grounds natural language text, queries, and privacy policies into a relational database to integrate, for the first time, contextual integrity and differential privacy over unstructured text . We introduce contextual differential privacy to reduce noise and a privacy aware Text to SQL method using Monte Carlo Tree Search that selects the lowest noise query in 75.3% of cases while achieving 0% leakage .	
3 SPARC: A Multi-Agent System for Electrical Circuit Question Answering	2026
Mushtari Sadia, Zhenning Yang, Umme Habiba Lamia, Nishat Shawrin, Ang Chen, Amrita Roy Chowdhury	
Under review at AAAI 2027 Project link	
Designed a multi-agent LLM system with orchestration that <i>answers questions on electrical circuit diagrams</i> by synthesizing and executing SPICE simulations. The system improves reliability and interpretability of multimodal LLM reasoning on this task and reaches 83% accuracy with up to 58% improvement over baselines.	

- 4 Trinqet: Private Triangle and Quadrangle Counting over Distributed Graphs** 2026
Mushtari Sadia, Amrita Roy Chowdhury
Under review at [NDSS 2027](#) | [Preprint](#)
Developed Trinqet, a privacy-preserving graph analytics system using the **MP-SPDZ** library, for triangle and quadrangle detection over distributed graphs with malicious security. Introduced MPC algorithms that exploit graph sparsity through differentially private noisy degree release, achieving $10^5 \times$ improvements in runtime.
- 5 Nomai: Single-Server Federated Learning with Private Weights** 2026
Yiyi Sun, Mushtari Sadia, Amrita Roy Chowdhury
Under review at [USENIX Security 2027](#)
Developed Nomai, a scalable MPC based federated learning system that provides data privacy, model privacy, and integrity for single server deployments with up to 10^6 users and can train MNIST in under $50ms$.
- 6 LogShield: A Transformer-based Advanced Persistent Threat Detection System Leveraging Self-Attention** 2022
Sihat Afnan, Mushtari Sadia*, Shahrear Iqbal, Anindya Iqbal (*equal contribution) | [Preprint](#)*

Workshop

- 7 Multi-modal Swarm Intelligence for Secure UAV Missions** 2024
Yunming Xiao, Mushtari Sadia, Ang Chen | [GenZero Workshop 2024](#) | [Poster](#)

Awards

- Microsoft Virtual Hackathon (2022) – 1st Runner Up** [GitHub](#)
Co-created an AI-based dengue forecast system using **MS Azure Services** to predict case counts in any region based on historical cases and weather parameters.
- HerWILL Datathon (2022) – Champion** [GitHub](#)
Developed a machine learning-based forecasting system for predicting taxi demand in urban areas.
- UNDP Women’s Digital Innovation Hackathon (2021) – 2nd Runner Up**
Built an AI-based Dengue Monitor & Control System.
- Fatima Fellowship:** 9-month predoctoral fellowship program where I worked with the MIT Camera Culture Group.
- Microsoft for Startups Founders Hub Membership:** Awarded \$3000 startup funding for AI-based dengue forecast system prototype built with MS Azure.
- GHC 22 Scholarship:** Merit-based scholarship to attend the Grace Hopper Celebration of Women in Computing.
- Dean’s List Scholarship (2018–2021):** Awarded for academic excellence during undergraduate studies.

Leadership Experience

- **President**, Bangladeshi Women in Computer Science & Engineering (BWCSE) (Apr 2022 – May 2023): coordinated programming contests, technical workshops, and seminars to for women in CS.
- **Batch Representative**, Bangladeshi Women in Computer Science & Engineering (BWCSE) (Apr 2021 – Apr 2022)

Technical Skills

Programming: Python, C, C++, Java, JavaScript, C#, SQL, Bash, CSS, LaTeX
ML / DL: PyTorch, TensorFlow, Keras, Scikit-learn, XGBoost, LightGBM, SciPy, CUDA libraries
Agentic Frameworks: LangGraph, LangChain, AutoGen, CrewAI
LLM Training / Fine-tuning: Hugging Face Transformers, PEFT, TRL, DeepSpeed, Accelerate
Data / Vision / Visualization: NumPy, Pandas, OpenCV, Matplotlib, Seaborn
Cloud / Dev / Deployment: AWS EC2, AWS S3, Google Cloud Platform, Git, Docker, W&B, vLLM
Web / Databases: React, Bootstrap, Django, Django REST, HTML, CSS, Node.js, MySQL, Oracle, SQLite
Systems / Security: NS3, xv6, MP-SPDZ, NTL