Afia Anjum

Email: afia.anjum70@gmail.com, axa2549@mavs.uta.edu, afia@lanl.gov
Contact no: +1 682 241 2633
Google Scholar || ResearchGate || LinkedIn || Website

Academic Qualification

Doctor of Philosophy in Computer Science *(Aug'21- May'26)*
Cyber-physical Systems Security Lab, University of Texas at Arlington (UTA), Texas, USA
CGPA: 4.00/4.00

Bachelor of Science in Computer Science and Engineering *(Feb'15- Dec'18)*
Military Institute of Science and Technology (MIST), Dhaka, Bangladesh
CGPA: 3.91/4.00 [Ranked **1st** in the Department; Recipient of the **MIST Medal** for Academic Excellence]

Research Interest

Wireless Communication, Semantic Communication, 5G/6G, Communication Security

Research Summary

I build secure and trustworthy AI-native communication systems for the next generation of cyber-physical infrastructure. My work spans wireless network security, semantic communication, and explainable AI, leveraging deep learning, large language models, and vision-language models to enhance the resilience, adaptability, and interpretability of connected systems — from autonomous vehicles and smart healthcare to smart grids.

Research Experience

Theoretical Division, Los Alamos National Laboratory, Los Alamos, New Mexico, USA. *(Jan'25 – Present)*
Graduate Researcher

- Developing deep reinforcement learning–based traffic rate control for black-box communication channels, enabling protocol-agnostic optimization where traditional congestion control methods fail.
- Built a network state forecasting–based defense framework for DDoS attacks, incorporating explainability methods to identify root causes and affected nodes, enabling proactive mitigation and enhanced resilience in Smart Grid communication systems.

University of Texas at Arlington, **Arlington, Texas, USA** *(Aug'21 – Present)*
Graduate Research Assistant and Project Lead

- Exposed inherent vulnerabilities in LLM–based Semantic Communication through text-driven adversarial attacks and explored defense strategies to secure intent-driven transmission in safety-critical systems.
- Designed adaptive, energy-aware resource allocation frameworks for next-generation 5G communication, supporting heterogeneous traffic with varying latency, reliability, and throughput requirements under constrained network conditions.
- Reimagined Internet architecture beyond traditional TCP/IP through data-centric paradigms such as Named Data Networking (NDN), enhancing their capabilities to support reliable, secure, and low-latency IoT communication.

Research Mentor – graduate and undergraduate students

- Developing vision language model (VLM)-driven reasoning frameworks for autonomous driving systems, enabling proactive intent prediction of the surrounding objects, cooperative multi-vehicle coordination, and real-time decision-making for safer connected transportation.
- Investigating adversarial vulnerabilities across model scales, analyzing attack transferability from large to small language models to advance secure and trustworthy AI deployment.
- Developed a quantitative evaluation framework for XAI methods used in AI-based clinical decision support systems to uncover inconsistencies, biases, and reliability gaps, guiding towards trustworthy clinical integration.

Intra-Lab Research Collaborations

- Co-developed standardized benchmarking and anomaly detection frameworks for intrusion detection in vehicular communication, enhancing reproducibility, model robustness, and trustworthiness in safety-critical systems.
- Contributed to exposing vulnerabilities across graph neural networks, knowledge distillation pipeline, and autonomous driving lane detection models through adversarial and data-driven attack analyses.
- Collaborated on developing privacy-preserving federated and split learning frameworks**,** enabling decentralized and personalized model adaptation in highly mobile environments.

Theoretical Division, Los Alamos National Laboratory, Los Alamos, New Mexico, USA. *(Jun'24 – Aug'24)*
Research Intern

- Developed Tensor Train Low-Rank Approximation (TT-LoRA), a parameter-efficient fine-tuning method that reduces the computational cost and environmental impact of LLMs while maintaining state-of-the-art performance. (*Best Paper Runner-up; Got selected for LANL press release*)

.

Teaching Experience

University of Texas at Arlington, **Arlington, Texas, USA** *(Aug'21 – Dec'24)*
Graduate Teaching Assistant

- Designed exams, quizzes, and assignments.
- Graded student submissions and provided detailed feedback.
- Supervised and mentored course projects, guiding students through design and implementation.
- Delivered lectures and managed classroom sessions in the instructor's absence.

Courses:

- *CSE 5344: Computer Networks*
- *CSE 5333/4333: Cloud Computing*
- *CSE 5306: Distributed Systems*
- *CSE 3313: Introduction to Signal Processing*

Upward Bound Math & Science Center, University of Texas at Arlington, Texas, USA *(Jun'23 – Jul'23)*
Web Development Instructor

- Taught a hands-on web development course to 17 high school students, covering HTML, CSS, and JavaScript.
- Students built new components each week, culminating in a fully functional final website.
- Organized students into teams to foster peer learning, problem-solving, and real-world project experience.

Military Institute of Science and Technology, Dhaka, Bangladesh *(Jan'19 – Jul'21)*
Lecturer

- Designed and conducted undergraduate courses and laboratory sessions.
- Created and evaluated assessments, including exams, quizzes, and assignments, to measure student learning.
- Supervised course projects, guiding students through design, implementation, and presentation.
- Mentored students in transforming course projects into research papers.

Courses:

- *CSE 460: Integrated Design Project / CapstoneProject - II*
- *CSE 360: Integrated Design Project / CapstoneProject - I*
- *CSE 323: Computer Architecture*
- *CSE 318: Data Communication Sessional*
- *CSE 310: Computer Network Sessional*
- *CSE 304: Compiler Sessional*
- *CSE 302: Database Management Systems Sessional*
- *CSE 216: Data Structures and Algorithms-II Sessional*
- *CSE 204: Data Structures and Algorithms-I Sessional*
- *CSE 105: Structured Programming Language*

Honors & Awards

- Invited speaker. *IEEE TCCN Rising Star Symposium Series 2025.*
- Travel Grant Award. *USENIX Security. 2025.*
- Best Paper Runner-up. *International Conference on Machine Learning and Applications (ICMLA) 2024.*
- Invited speaker. *Named Data Networking Community Meeting (NDNComm) 2024.*
- Travel Grant Award. *Network and Distributed System Security Symposium (NDSS) 2024.*
- Best Ph.D. Lightning Talk Award. *Student Computing Research Festival (SCRF) 2024, UTA.*
- NSF Student Travel Award. *Cyber-Physical Systems and Internet-of-Things Week (CPS-IoT Week) 2023.*

- Ph.D. Lightning Talk Award (2nd Runner-up). *Student Computing Research Festival (SCRF) 2023, UTA.*
- Best Paper Award. *International Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022.*
- Travel Grant Award. *CyberTruck Challenge 2022.*
- Travel Grant Award. *IEEE S&P 2022.*
- Ph.D. Lightning Talk Award (Runner-up). *Student Computing Research Festival (SCRF) 2022, UTA.*
- MIST Medal for securing the 1st position in the department. *Military Institute of Science and Technology. 2018.*
- Got selected for the Dean's List Award. *Military Institute of Science and Technology. 2015-2018.*

Publications

Conferences:

- **Anjum A**, Lawrence N, Olufowobi H. Modeling DDoS Impact in IoT Networks: A Comprehensive Analysis of Time-Series Models and Explainability Strategies. (Under review) ***NDSS 2027***

- **Anjum A,** S. Siddhant, Mitra A, Agbaje P, Olufowobi H. LLM-RA: Prompt-Adaptive 5G NR Resource Allocation via Reinforcement-Guided Language Models. (Under review) ***MobiHoc 2027***

- Agbaje P, **Anjum A**, Mitra A, Olufowobi H. Unveiling Graph Copycats: Inference Attacks with Student Models. (in press) ***PoPETS 2026***

- **Anjum A,** Mitra A, Agbaje P, Alam MA, Roy D, Parwez MS, Olufowobi H. SemPerGe: Unveiling Text-based Adversarial Attacks on Semantic Communication. ***CNS 2025***

- Mitra A, **Anjum A,** Paul Agbaje, Pese M, Olufowobi H. FedVLM: Scalable Personalized Vision-Language Models through Federated Learning. ***ECAI 2025***

- Mitra A, MohajerAnsari P, **Anjum A**, Agbaje P, Pese M, Olufowobi H. Beyond the Glow: Understanding Luminescent Marker Behavior Against Autonomous Vehicle Perception Systems. ***USENIX VehicleSec 2025***

- **Anjum A,** Eren ME, Boureima I, Alexandrov B, Bhattarai. Tensor Train Low-rank Approximation (TT-LoRA): Democratizing AI with Accelerated LLMs. ***ICMLA 2024***

- Agbaje P, **Anjum A**, Zahidur T, Islam M, Nwafor E, Olufowobi H. FedCime: An Efficient Federated Learning Approach For Clients in Mobile Edge Computing. **EDGE 2023**

- **Anjum A**, Hounsinou S, Olufowobi H. Work-in-Progress: Deadline-Aware Named Data Networking for Time-Sensitive IoT Applications. ***RTAS 2023***

- Agbaje P, **Anjum A**, Mitra A, Hounsinou S, Olufowobi H. Privacy-Preserving Intrusion Detection System for Internet of Vehicles using Split Learning. ***BDCAT 2023***

- **Anjum A**, Olufowobi H. Towards Mitigating Blackhole Attack in NDN-Enabled IoT. ***ICCE 2023***

- **Anjum A**, Agbaje P, Hounsinou S, Olufowobi H. In-Vehicle Network Anomaly Detection Using Extreme Gradient Boosting Machine. ***MECO 2022***

- **Anjum A**, Olufowobi H. Poster: Mitigating Blackhole Attack in NDNoT. ***IEEE S&P 2022***

- Agbaje P, **Anjum A**, Mitra A, Bloom G, Olufowobi H. A Framework for Consistent and Repeatable Controller Area Network IDS Evaluation. ***AutoSec 2022***

Journals:

- **Anjum A**, Agbaje P, Mitra A, Hounsinou S, Olufowobi H. Optimizing Resource Allocation for Multi-hop Sidelink Communication in 5G-NR. (under review) **(IF: 8.4)** ***IEEE T-ITS***

- **Anjum A,** Yousaf A, Mitra A, Agbaje P, Coffee M, Olufowobi H. (2025) Systematization and Empirical Evaluation of Explainable AI Methods for Clinical Decision Support Systems. **(IF: 8.0)** (under review) ***ACM HEALTH***

- **Anjum A**, Agbaje P, Hounsinou S, Guizani N, Olufowobi H. (2024) D-NDNoT: Deterministic Named Data Networking for Time-Sensitive IoT Applications. **(IF: 8.9)** ***IEEE IoT-J***

- **Anjum A**, Oseghale E, Mitra A, Agbaje P, Nwafor E, Olufowobi H. (2024) Towards NDN Technology: Emerging Applications, Use Cases, and Challenges for Secure Data Communications. **(IF: 6.1)** ***FGCS***

- Agbaje P, **Anjum A**, Mitra A, Oseghale E, Bloom G, Olufowobi H. (2022) Survey of Interoperability Challenges in the Internet-of-Vehicles. **(IF: 8.4)** ***IEEE TITS***

Presentations and Talks

- "Words Under Attack: Exposing Vulnerabilities in Text-driven Semantic Communication" – *Invited Talk, Rising Start Symposium'25, IEEE TCCN Special Interest Group for AI/ML Learning in Security (virtual).*
- "Tensor Train Low-rank Approximation (TT-LoRA): Democratizing AI with Accelerated LLMs" – *Paper Presentation, ICMLA'24, Miami, Florida, USA.*
- "Poster: Tensor Train Low-rank Approximation (TT-LoRA): Democratizing AI with Accelerated LLMs" – *Student Symposium'24, Los Alamos National Laboratory, Los Alamos, New Mexico, USA.*
- "D-NDN: Deterministic Named Data Networking for Time-Sensitive Applications using Deadline-based Dynamic Scheduling" – *Invited talk, NDNComm'24, Washington DC, USA.*
- Explainability in Clinical Decision Support Systems for Interpretability, Trustworthiness, and Usability" – *PhD Lightning Talk, SCRF'24, UTA, Texas, USA.*
- "Work-in-Progress: Deadline-Aware Named Data Networking for Time-Sensitive IoT Applications" – *Paper Presentation, RTAS'23, San Antonio, Texas, USA.*
- "In-Vehicle Network Anomaly Detection Using Extreme Gradient Boosting Machine" – *Paper Presentation, MECO'23 (virtual).*
- **"**When Speed Lies: Compromising Accelerator Dashboards to Mislead Drivers" – *Workshop Presentation, CyberTruck Challenge'22, Warren, Michigan, USA.*
- "Poster: Mitigating Blackhole Attack in NDNoT" – *IEEE S&P'22, San Francisco, California, USA.*

Academic Service

Reviewer

- IEEE Internet of Things Journal (IoT-J)
- International Joint Conference on Artificial Intelligence (IJCAI)
- Real-time Systems Symposium (RTSS)
- International Conference on Learning Representations (ICLR)
- IEEE Global Communications Conference (Globecom)

Volunteer

- Student volunteer at NDSS Vehicle Security and Privacy (VehicleSec), San Diego, California, USA. 2024
- Conducted workshop at OurCS@DFW, UTA. 2022, 2023, 2024

Attendee

- Named Data Networking Community Meeting (NDNComm). Washington DC, USA. 2024
- CPS-IoT Week, San Antonio, Texas, USA. 2023
- STARS Celebration. Dallas, Texas, USA. 2023
- CyberTruck Challenge, Warren, Michigan, USA. 2022

Skills

Programming Languages : Python, PyTorch, TensorFlow, C++, JavaScript, SQL, PHP, HTML, CSS, Socket
Professional Software : NS2, NS3, OMNet++, MATLAB, WireShark, MySQL, Oracle, Firebase