

Afia Anjum, PhD

Assistant Professor

Department of Computer Science

Texas Christian University

Email: afia.anjum@tcu.edu

Contact no: +1 682 241 2633

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

Academic Appointments

Assistant Professor

(Aug'26- Present)

Department of Computer Science

Texas Christian University, Fort Worth, Texas, USA

Faculty Researcher (Guest)

(Aug'26- Present)

Advanced Research in Cyber Systems Division

Los Alamos National Laboratory, Los Alamos, New Mexico, USA

Education

Ph.D. in Computer Science

(Aug'21- May'26)

Cyber-physical Systems Security Lab

University of Texas at Arlington (UTA), Arlington, Texas, USA

Dissertation: "Optimizing the Frontier: Enhancing Security and Efficiency of Wireless Communication Systems for Internet of Things"

Advisor: Dr. Habeeb Olufowobi

B.Sc. in Computer Science and Engineering

(Feb'15- Dec'18)

Military Institute of Science and Technology (MIST), Dhaka, Bangladesh

Thesis: "Construction of Connected Dominating Set to Reduce Contention in Wireless Ad-hoc Network"

Advisor: Chowdhury Nawrin Ferdous

Research Interests

Security of AI-driven communication systems; adversarial threats to semantic and learned-representation-based communication; trustworthy and resilient wireless communication; cyber-physical systems security across IoT, autonomous vehicles, and smart grids; real-time systems; and machine learning for security.

Research Experience

Theoretical Division, Los Alamos National Laboratory, NM, USA

(Jan'25 – Jul'26)

Graduate Researcher

- Developed deep reinforcement learning-based traffic rate control for black-box communication channels, enabling protocol-agnostic optimization where traditional congestion control fails.
- 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 – May '26)

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 LLM-based 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

- Developed 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.
- Investigated 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, NM, 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)

Honors & Awards

- Invited speaker. *IEEE TCCN Rising Star Symposium Series* 2025.
- Rising Star Award 2025, *IEEE Technical Committee on Cognitive Networks (TCCN)*.
- Travel Grant Award. *USENIX Security*. 2025.
- Best Paper Runner-up. *International Conference on Machine Learning and Applications*, 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*, 2023.
- Ph.D. Lightning Talk 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 Runner-up. *Student Computing Research Festival (SCRF)* 2022, UTA.
- MIST Medal for securing the 1st position in the department. *MIST*. 2018.
- Dean's List Award. *Military Institute of Science and Technology*. 2015-2018.

Publications

Journals:

- **Anjum, A.**, Lawrence, N., & Olufowobi, H. "Forecasting DDoS-Induced Network Degradation: An Empirical Study of Time-Series Models." *Journal of Network and Computer Applications*. (to be submitted)
- Mitra, A., Saeed, S., **Anjum, A.**, Agbaje, P., & Olufowobi, H. "Adversarial Analysis of Autonomous Vehicular Perception Systems." *ACM Computing Surveys*. (under review)
- Agbaje, P., Ladhari, M., Chumo, J., Saeed, S., Mitra, A., **Anjum, A.**, & Olufowobi, H. "Security Strategies for Graph Neural Networks." *ACM Computing Surveys*. (under review)
- **Anjum, A.**, Yousaf, A., Mitra, A., Agbaje, P., Coffee, M., & Olufowobi, H. "Explainable AI for Clinical Decision Support Systems: A Systematic Review with Empirical Evaluation." *ACM Transactions on Computing for Healthcare*. (under review)
- **Anjum, A.**, Oseghale, E., Mitra, A., Agbaje, P., Nwafor, E., & Olufowobi, H. "Towards NDN Technology: Emerging Applications, Use Cases, and Challenges for Secure Data Communications." *Future Generation Computer Systems (FGCS)*, 151, pp.12-31, 2024.
- **Anjum, A.**, Agbaje, P., Hounsinnou, S., Guizani, N., & Olufowobi, H. "D-NDNoT: Deterministic Named Data Networking for Time-Sensitive IoT Applications." *IEEE Internet of Things Journal*, 11(14), pp.24872-24885, 2024.
- Agbaje, P., **Anjum, A.**, Mitra, A., Oseghale, E., Bloom, G., & Olufowobi, H. "Survey of Interoperability Challenges in the Internet-of-Vehicles." *IEEE Transactions on Intelligent Transportation Systems*, 23(12), pp.22838-22861, 2022.

Conferences:

- **Anjum, A.**, Shettiwar, S., Mitra, A., Agbaje, P., & Olufowobi, H. “LLM-RA: Prompt-Adaptive 5G NR Resource Allocation via Reinforcement-Guided Language Models”. *27th International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc)*, 2026. (under review)
- Mitra, A., **Anjum, A.**, Agbaje, P., & Olufowobi, H. “FedMoEFlow: A Framework For Mixture-of-Experts Based Generative Models Using Federated Learning”. *IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*, 2027. (under review)
- Mitra, A., Sharma, K., Alam, A., **Anjum, A.**, Agbaje, P., Parwez, S., Nwafor, E., & Olufowobi, H. “RF-VLM: mmWave-Aided Vision-Language Models for Indoor Scene Understanding and Navigation.” *IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*, 2027. (under review)
- Yousaf, A., Agbaje, P., **Anjum, A.**, Mitra, A., & Olufowobi, H. “Towards Enhanced Sparse-View Tomographic Reconstruction Using 3D Gaussian Splatting.” *IEEE International Conference on 3D Vision (3DV)*, 2026.
- Agbaje, P., **Anjum, A.**, Mitra, A., & Olufowobi, H. “Unveiling Graph Copycats: Inference Attacks with Student Models.” *Proceedings on Privacy Enhancing Technologies (PoPETS)*, 2026.
- Agbaje, P., Mitra, A., **Anjum, A.**, Khose, P., Nwafor, E., & Olufowobi, H. “A Collaborative Distillation Framework for Graph Neural Networks.” *European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN)*, 2026.
- **Anjum, A.**, Mitra, A., Agbaje, P., Alam, M. A., Roy, D., Parwez, M. S., & Olufowobi, H. “SemPerGe: Unveiling Text-based Adversarial Attacks on Semantic Communication.” *IEEE Conference on Communications and Network Security (CNS)*, 2025.
- Mitra, A., **Anjum, A.**, Agbaje, P., Pese, M., & Olufowobi, H. “FedVLM: Scalable Personalized Vision-Language Models through Federated Learning.” *European Conference on Artificial Intelligence (ECAI)*, 2025.
- Yousaf, A., Mitra, A., Agbaje, P., **Anjum, A.**, & Olufowobi, H. “DAPS-AGF: Depth-Aware Perceptual Similarity with Adaptive Gradient Filtering for Enhanced Outdoor Scene Reconstruction.” *IEEE/CVF International Conference on Computer Vision*, 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 Symposium on Vehicle Security and Privacy (VehicleSec)*, 2025.
- **Anjum, A.**, Eren, M. E., Boureima, I., Alexandrov, B., & Bhattarai, M. “Tensor Train Low-rank Approximation (TT-LoRA): Democratizing AI with Accelerated LLMs.” *IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2024. Best Paper Runner-up.
- Agbaje, P., **Anjum, A.**, Zahidur, T., Islam, M., Nwafor, E., & Olufowobi, H. “FedCime: An Efficient Federated Learning Approach for Clients in Mobile Edge Computing.” *IEEE International Conference on Edge Computing (EDGE)*, 2023.
- **Anjum, A.**, Hounsinnou, S., & Olufowobi, H. “Work-in-Progress: Deadline-Aware Named Data Networking for Time-Sensitive IoT Applications.” *IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)*, 2023.

- Agbaje, P., **Anjum, A.**, Mitra, A., Hounsinnou, S., & Olufowobi, H. “Privacy-Preserving Intrusion Detection System for Internet of Vehicles using Split Learning.” *IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT)*, 2023.
- **Anjum, A.**, & Olufowobi, H. “Towards Mitigating Blackhole Attack in NDN-Enabled IoT.” *IEEE International Conference on Consumer Electronics (ICCE)*, 2023.
- **Anjum, A.**, Agbaje, P., Hounsinnou, S., & Olufowobi, H. “In-Vehicle Network Anomaly Detection Using Extreme Gradient Boosting Machine.” *Mediterranean Conference on Embedded Computing (MECO)*, 2022.
- Agbaje, P., **Anjum, A.**, Mitra, A., Bloom, G., & Olufowobi, H. “A Framework for Consistent and Repeatable Controller Area Network IDS Evaluation.” *Workshop on Automotive and Autonomous Vehicle Security (AutoSec)*, 2022. Best Paper Award.
- **Anjum, A.**, & Olufowobi, H. “Poster: Mitigating Blackhole Attack in NDN-T.” *IEEE Symposium on Security and Privacy (S&P)*, 2022

Teaching Experience

Assistant Professor – Texas Christian University

(Aug’26 – Present)

Courses:

- COSC 30503: Systems Programming (Fall’26)

Graduate Teaching Assistant - University of Texas at Arlington

(Aug’21 – Dec’24)

Courses:

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

Web Development Instructor - Upward Bound Math & Science Center, UTA

(Jun’23 – Jul’23)

- Taught a hands-on web development course to 17 high school students, covering HTML, CSS, and JavaScript, culminating in a functional final website built in teams.

Lecturer - Military Institute of Science and Technology, Dhaka, Bangladesh

(Jan’19 – Jul’21)

Courses:

- CSE 460: Integrated Design Project / Capstone Project - I
- CSE 360: Integrated Design Project / Capstone Project - II
- 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

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 NDN-T” – *IEEE S&P’22, San Francisco, California, USA*.

Academic Service

Technical Program Committee

- MobiArch Workshop, ACM International Conference on Mobile Computing and Networking (MobiCom), 2026.
- EAI International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles (SmartSP), 2026.

Reviewer

- IEEE Internet of Things Journal (IoT-J), 2024–present
- IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2027
- International Joint Conference on Artificial Intelligence (IJCAI), 2026
- IEEE Real-Time Systems Symposium (RTSS), 2025
- IEEE Global Communications Conference (Globecom), 2025
- International Conference on Learning Representations (ICLR), 2024