# Arkajyoti Mitra

Email | LinkedIn | Google Scholar | Website

## Education

**University of Texas at Arlington (UTA)**, Texas, USA — Fall'20 – Fall'25 (expected)
Doctor of Philosophy, Computer Science — GPA: 3.9/4.0

**Indian Institute of Technology (IIT)**, Dhanbad, India — Fall'17 – Spring'19
Master of Technology, Computer Science and Engineering — CGPA: 8.65/10.0

## Research Interest

Autonomous Vehicular Perception Systems, Scene Understanding, Vision-Language Models (VLM), Gaussian Splatting, Flow-Matching, Diffusion, Generative Modeling, 3D Reconstruction, Computer Vision Applications, Adversarial Attack, Multimodal Learning, Federated Learning, Reinforcement Learning, Systems Security, Network Security, Vehicular Security, Vision Security, LLM/VLM Security.

## Publications

### Conferences, Journals, and Workshops

- **Arkajyoti Mitra**, Afia Anjum, Paul Agbaje, Mert D. Pesé, Habeeb Olufowobi; **FedVLM: Scalable Personalized Vision–Language Models through Federated Learning**, *European Conference on Artificial Intelligence (ECAI)*, 2025. [Accepted]
- **Arkajyoti Mitra**, Pedram MohajerAnsari, Afia Anjum, Paul Agbaje, Mert D. Pesé, Habeeb Olufowobi; **Beyond the Glow: Understanding Luminescent Marker Behavior Against Autonomous Vehicle Perception Systems**, *3rd USENIX Symposium on Vehicle Security and Privacy (VehicleSec'25)*, pp. 195–210, 2025.
- Afia Anjum, **Arkajyoti Mitra**, Paul Agbaje, Md Ahanaful Alam, Debashri Roy, Md Salik Parwez, Habeeb Olufowobi; **SemPerGe: Unveiling Text-based Adversarial Attacks on Semantic Communication**, *IEEE Conference on Communications and Network Security (CNS)*, 2025. [Accepted]
- Aqsa Yousaf, **Arkajyoti Mitra**, Paul Agbaje, Afia Anjum, Habeeb Olufowobi; **DAPS-AGF: Depth-Aware Perceptual Similarity with Adaptive Gradient Filtering for Enhanced Outdoor Scene Reconstruction**, *End-to-End 3D Learning (ICCV Workshop)*, 2025. [Accepted]
- Paul Agbaje, A. Mookhoek, Afia Anjum, **Arkajyoti Mitra**, Mert D. Pesé, Habeeb Olufowobi; **AutoWatch: Learning Driver Behavior with Graphs for Auto Theft Detection and Situational Awareness**, *2nd ISOC Symposium on Vehicles Security and Privacy (VehicleSec)*, 2024.
- Afia Anjum, Paul Agbaje, **Arkajyoti Mitra**, E. Oseghale, E. Nwafor, Habeeb Olufowobi; **Towards Named Data Networking Technology: Emerging Applications, Use Cases, and Challenges for Secure Data Communication**, *Future Generation Computer Systems*, vol. 151, pp. 12–31, 2024.
- Paul Agbaje, Afia Anjum, **Arkajyoti Mitra**, S. Hounsinou, E. Nwafor, Habeeb Olufowobi; **Privacy-Preserving Intrusion Detection System for Internet of Vehicles using Split Learning**, *IEEE/ACM 10th International Conference on Big Data Computing, Applications and Technologies (BDCAT)*, 2023.
- Paul Agbaje, Afia Anjum, **Arkajyoti Mitra**, E. Oseghale, Gedare Bloom, Habeeb Olufowobi; **Survey of Interoperability Challenges in the Internet of Vehicles**, *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 22838–22861, 2022.
- Paul Agbaje, Afia Anjum, **Arkajyoti Mitra**, Gedare Bloom, Habeeb Olufowobi; **A Framework for Consistent and Repeatable Controller Area Network IDS Evaluation**, *Fourth International Workshop on Automotive and Autonomous Vehicle Security (AutoSec)*, 2022. ***[Best Paper Award]***
- **Arkajyoti Mitra**, P. C. Tripathi, S. Bag; **Identification of Astrocytoma Grade using Intensity, Texture, and Shape Based Features**, *Soft Computing for Problem Solving: SocProS 2018, vol. 1*, pp. 455–465, 2019.

## In Submission

- **Arkajyoti Mitra**, Kopil Sharma, Md Ahanaful Alam, Afia Anjum, Paul Agbaje, Md Salik Parwez, Ebelechukwu Nwafor, Habeeb Olufowobi; **RF-VLM: mmWave Aided Vision–Language Model for Autonomous Indoor Navigation**, *In Submission*.
- **Arkajyoti Mitra**, Paul Agbaje, Afia Anjum, Habeeb Olufowobi; **FedMoeFlow: Scaling Mixture-of-Experts Based Generative Models Through Federated Learning**, *In Submission*.
- **Arkajyoti Mitra** Md Sufyaan Saeed, Afia Anjum, Paul Agbaje, Habeeb Olufowobi; **SoK: Adversarial Analysis of Autonomous Vehicular Perception Systems**, *In Submission*.
- Paul Agbaje, **Arkajyoti Mitra**, Afia Anjum, P. Khose, E. Nwafor, Habeeb Olufowobi; **Enhancing Graph Neural Networks: A Mutual Learning Approach**, *In Submission*.
- Paul Agbaje, Afia Anjum, **Arkajyoti Mitra**, Habeeb Olufowobi; **Unveiling Graph Copycats: Inference Attacks with Student Models**, *In Submission*.
- Paul Agbaje, Myriyam Ladhari, Jesse Chumo, Afia Anjum, Habeeb Olufowobi; **SoK: Security Strategies for Graph Neural Networks**, *In Preparation*.
- Afia Anjum, Paul Agbaje, **Arkajyoti Mitra**, Sena Hounsinou, Md Salik Parwez, Habeeb Olufowobi; **Optimizing Resource Allocation for Multi-hop Sidelink Communication in 5G-NR**, *In Submission*.
- Afia Anjum, Aqsa Yousaf, **Arkajyoti Mitra**, Paul Agbaje, Megan Coffee, Habeeb Olufowobi; **Systematization and Empirical Evaluation of Explainable AI Methods for Clinical Decision Support Systems**, *In Submission*.
- Aqsa Yousaf, Paul Agbaje, Afia Anjum, **Arkajyoti Mitra**, Habeeb Olufowobi; **Towards Enhanced Sparse-View Tomographic Reconstruction Using 3D Gaussian Splatting**, *In Submission*.
- Pedram MohajerAnsari, A. Domeke, J. de Voor, **Arkajyoti Mitra**, G. Johnson, A. Salarpour, et al.; **Discovering New Shadow Patterns for Black-Box Attacks on Lane Detection of Autonomous Vehicles**, 2024. *In Submission*

## Research Projects & Experience

**Vision–Language Models (VLM)** Ongoing

- Developing VLMs for multimodal reasoning and cross-sensor integration for unknown-terrain AV navigation.
- Developing a scalable framework for VLM training.
- Fine-tuning VLMs on VQA benchmark datasets (OK-VQA, TextVQA, GSM100K).

**3D Reconstruction** Ongoing

- Building digital twin environments using 3DGS for safer development of autonomous driving.
- Hyperparameter tuning for scene reconstruction; improving quality while reducing memory footprint.

**Generative Modelling** Ongoing

- Building flow-matching models to learn velocity fields for efficient point-cloud generation.
- Developing a scalable framework for diffusion-based models.

**Adversarial Analysis of Lane and Drivable Space Detection Models** Jan. 2024 – Aug. 2025

- Developed digital setup for simulation-based analysis of adversarial threats.
- Built physical testbed for real-world analysis of adversarial threats.
- Proposed a novel attack vector against SOTA models (YOLOPv2, CLRerNet, TwinLiteNet).

**MITRE eCTF Competition (Entered Design Phase)** Jan. 2025 – Apr. 2025

- Led a team to develop a secure satellite TV system using the MAX78000FTHR board.

**MITRE eCTF Competition (Entered Attack Phase)** Jan. 2024 – Apr. 2024

- Led a team to develop a secure medical device using the MAX78000FTHR board.

**CyberTractor Workshop** July 2022 – July 2022

- Secured second position by identifying/patching a security vulnerability on CAN via replay attacks.

**CyberTruck Workshop** June 2022 – June 2022

- Developed a spoofing attack on the CAN, compromising vehicular components (brakes, fuel indicators).

**Computer-Aided Identification of Astrocytoma Tumor Grades using Brain MRI** June 2018 – May 2019

- Developed a framework that detects and classifies brain tumors from MRI scans.

## Technical Skills

**Programming & Software:** Python, MATLAB, C++, C, CARLA (simulator)

**ML Frameworks:** PyTorch, TensorFlow, Diffusers, Transformers

## Work Experiences

**Graduate Teaching Assistant / Research Assistant**, University of Texas at Arlington (UTA), Texas, USA Aug. 2020 – Present

- Research focus: applying VLMs for autonomous driving and improving latent representations for seamless navigation; conducted in the Cyber-Physical System Security (CSS) Lab.
- Collaborate on projects, review and write research papers, and mentor undergraduate and master's students; strengthened communication, critical thinking, and time/resource management.

**Teaching Assistant**, Indian Institute of Technology (IIT) Dhanbad, India July 2018 – May 2019

- Assisted multiple instructors across varied courses and environments, gaining broad instructional experience.

## Awards and Scholarships

- Travel grant to attend VehicleSec'25 Aug. 2025
- Summer Research Fellowship at UTA June 2025
- Travel grant to attend VehicleSec'24 Feb. 2024
- Travel grant to attend TAPIA'23 Sept. 2023
- Travel grant to attend CyberTractor Workshop June 2022
- Travel grant to attend CyberTruck Workshop July 2022
- Best Paper Award at AutoSec'22 Apr. 2022
- Second Best Paper Award, Computer Society of India (CSI), Kolkata Aug. 2016

## Other Activities

- Volunteered for VehicleSec'24
- Volunteered for SC'22