PRETOM ROY OVI

3925 N Elm Street, Apt 1423, Denton, TX 76207
+1(443)248-9841 ⋄ pretomroy.ovi@unt.edu ⋄ LinkedIn ⋄ Google Scholar

EDUCATION

Ph.D. in Information Systems *January 2020 - July, 2024*
University of Maryland, Baltimore County (UMBC)

M.Sc. in Information Systems *January 2020 - December 2021*
University of Maryland, Baltimore County (UMBC)

B.Sc. in Computer Science and Engineering *May 2012 - February 2017*
Bangladesh University of Engineering and Technology (BUET)

WORK EXPERIENCE

Tenure Track Assistant Professor August 2024 - Present
Department of Data Science
University of North Texas

Research Assistant August 2021 - July 2024
Center for Real-time Distributed Sensing and Autonomy (CARDS)
University of Maryland, Baltimore County (UMBC)

Graduate Teaching Assistant August 2020 - July 2021
Department of Information Systems
University of Maryland, Baltimore County (UMBC)

Graduate Research Assistant January 2020 - July 2020
Database Lab
University of Maryland, Baltimore County (UMBC)

Software Engineer August 2018 - September 2019
Ctrends Software and Services Ltd.

RESEARCH DOMAINS

Dissertation Topic: A Robust Federated Learning Framework against Cyber Intrusions to Ensure Data Confidentiality and Model Integrity.

- Addressed data confidentiality challenges in AI/ML posed by adversarial attacks, including gradient inversion attacks, data reconstruction attacks as well as membership inference attacks.
- Developed effective defense strategies, including quantized privacy risk measurement, differential privacy, secure aggregation, and secure multi-party computation.
- Addressed malicious influence, backdoor insertion and bias introduction to machine learning models caused by model poisoning attacks, data poisoning attacks and evasion attacks. Also developed robust defenses to maintain the purity and integrity of the machine learning models from training phase to inference stage.

Research Interest: Cyber Security, Privacy Preserving AI, Wireless Communication, Power Electronics and Edge Computing.

PUBLICATIONS

- **Mixed Quantization Enabled Federated Learning to Tackle Gradient Inversion Attacks**
  Author: Pretom Roy Ovi, Emon Dey, Nirmalya Roy, A Gangopadhyay
  Venue: Proceedings of IEEE/CVF Conf. on Computer Vision and Pattern Recognition (CVPR), 2023.
- **Revealing Security Risks in Audio Recognition Systems via Gradient Inversion Attacks**
  Author: Pretom Roy Ovi, A Gangopadhyay
  Venue: IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2024
- **Secured Federated Training: Detecting Compromised Nodes and Identifying the Type of Attacks**
  Author: Pretom Roy Ovi, A Gangopadhyay, Robert F. Erbacher, Carl Busart
  Venue: 21st IEEE International Conference on Machine Learning and Applications (ICMLA), 2022.

- **Towards Developing Data Security Aware Federated Learning for Multimodal Contested Environment**
  Author: Pretom Roy Ovi, Emon Dey, N Roy, A Gangopadhyay Best Paper Award
  Venue: Artificial Intelligence and Machine Learning for Multi-Domain Operations, SPIE, 2022.
- **Confident Federated Learning to Tackle Label Flipped Data Poisoning Attacks**
  Author: Pretom Roy Ovi, A Gangopadhyay Best Paper Award
  Venue: In Artificial Intelligence and Machine Learning for Multi-Domain Operations, SPIE, 2023.
- **A Comprehensive Study of Gradient Inversion Attacks in Federated Learning and Baseline Defense Strategies**
  Author: Pretom Roy Ovi, A. Gangopadhyay
  Venue: 2023 57th Annual Conference on Information Sciences and Systems (CISS), 2023.
- **ARIS: A Real-Time Edge Computed Accident Risk Inference System**
  Author: Pretom Roy Ovi, Emon Dey, N Roy, A Gangopadhyay.
  Venue: In 2021 IEEE International Conference on Smart Computing, IEEE Computer Society.
- **TinyM2Net: A Flexible System Algorithm Co-designed Multimodal Learning Framework for Tiny Devices**
  Author: Hasib-al-Rashid, Pretom Roy Ovi, Carl Busart, A Gangopadhyay
  Venue: TinyML Research Symposium 2022.
- **Generative Adversarial Domain Adaptation Network For Debris Detection Using Drone**
  Venue: 2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS).

PROJECTS

Robotic Sensing, Navigation, and Perception (funded by U.S. Army Grant No. W911NF21-20076)
This project focuses on enabling autonomous navigation and communication among a swarm of UGVs (Unmanned Ground Vehicles), including Spot Robots (legged robots) from Boston Dynamics, as well as Jackal and Husky (wheeled robots) from Clearpath Robotics. These robots work together in a coordinated manner to achieve common goals. Each robot is equipped with Velodyne VLP-16 lidar for rapid environment scanning and detailed 3D mapping, facilitating autonomous navigation. Additionally, the Robot Operating System (ROS) is utilized to enable intercommunication among the robots, such as transmitting commands from a master to slaves.

Algorithm Development for MM Wave Radar to Detect Object and its Movement on Fully Obfuscated areas (funded by U.S. Army Grant No. W911NF21-20076)
High-frequency signals have the ability to penetrate certain types of obstacles like fog, rain, dust, clothing, and drywall. The Doppler effect causes frequency shifts in radar signals when objects are in motion. By analyzing these frequency shifts, we build an algorithm that can determine the moving object and its direction in completely obfuscated areas, which we demonstrate in ArtIAMAS field experiments in Gracies Quarter, 2023. Our signal processing pipeline involves a wavelet denoiser, pulse Doppler filter, and peak detection algorithm.

Causal GAN for Counterfactual Image Generation
The aim is to generate counterfactual images utilizing Causal GAN. We considered three aspects of the image: the texture of the object, the shape of the object, and the background as the causation image generation process. By using the causalGAN, we generate counterfactual images by interchanging the texture, shape, and background among objects in the image.

AI on the Edge
The goal is to build a machine learning algorithm with multi-modal fusion (image and audio) for object detection, scene classification and finally AI model deployment on robotic platform and/or resource constrained edges such as Raspberry Pi and Jetson Nano.

TEACHING EXPERIENCE

Instruct Graduate Course *DTSC 5505: Applied Machine Learning for Data Scientists*

As Teaching Assistant:

- Introduction to Data Mining
- Statistical Analysis and Machine Learning

List of Supervised Undergraduate Students:

- Afolarin Abe (CSEE)
- Aaron Chiu (IS)
- Liam Mackinno (IS)
- Dhruvi Patel (IS)
- Jason Chen (IS)
- Jonathan Harwood (IS)
- Shaniah Reece (ME)
- Alpha Bayoh (IS)
- Luther Daigle (IS)
- Adil Mohammad (Biology)
- Ben Polyakov (IS)
- Anu Joy (IS)
- Hong Nguyen (IS)
- Olisa Okolo(Business)
- Jalwa Ihsan (Business)
- Zainab Siddiqui (CSEE)
- Zainab Shaikh (IS)
- Niyati Rami (IS)
- Ayu Fantaw (CSEE)

TECHNICAL STRENGTHS

Programming Language:	Python, SQL (Oracle), C, C++, R, Assembly language, HTML
Deep Learning Framework:	Tensorflow, Pytorch and familiar with CNN, GAN, LSTM, Transformer
Machine Learning Algorithm:	Logistic Regression, Decision Tree, Clustering, KNN, Random Forest
Machine Learning Library:	Numpy, Pandas, Q-Keras, Matplotlib, SciKit-Learn, NLTK, Librosa
Hardware Proficiency:	Raspberry Pi, Jetson Nano, Jetson Xavier, Google Coral Dev Board

AWARDS AND PROFESSIONAL ACTIVITIES

- Best Paper Award at SPIE Defence and Commercial Sensing Conference'22 and awarded with $1000.
- Awarded with Best Student Paper at SPIE Defence and Commercial Sensing Conference'23 and awarded with $1000.
- Project on"Robotic Sensing and Perception" got featured on CBS News, Baltimore.
- Achieved student travel grant for attending workshops and conferences from NSF HDR DSC (Harnessing Data Revolution) grant No. 1923982 ($2125).
- Achieved student travel grant for attending conferences from ArtIAMAS cooperative agreement, U.S. Army Grant No. W911NF21-20076 ($4250).
- Registered sub-reviewer of PMC journal, IEEE ICDM.
- Served as a mentor to supervise undergrad students funded by NSF HDR DSC (Harnessing Data Revolution) grant No. 1923982.
- Student member of the Society of Photo-Optical Instrumentation Engineers (SPIE).
- Presented research papers at multiple venues i.e., CVPR'23, SPIE'23, IEEE CISS'23, ICMLA'22, SPIE'22, IEEE SMARTCOMP'21.