Pretom Roy Ovi

povi1@umbc.edu | (443)-248-9841 | pretom-roy-ovi-258603237 | Baltimore, Maryland

Education

Doctor of Philosophy (PhD) — *AI/ML Privacy & Security* January 2020 - April 2024
University of Maryland, Baltimore County CGPA: 3.94/4.00
Dissertation Title: Developing Robust Machine Learning Framework against Cyber Intrusions to Preserve User Privacy and Ensure Data Confidentiality.

Master of Science — *Computer and Information Systems* January 2020 - December 2021
University of Maryland, Baltimore County CGPA: 3.94/4.00

Bachelor of Science — *Computer Science and Engineering* May 2012 - February 2017
Bangladesh University of Engineering and Technology (BUET) CGPA: 3.26/4.00

Skills

Programming Languages: Python, R, C, C++, SQL (Oracle), Assembly language, HTML
Machine/Deep Learning Frameworks: Tensorflow, Keras, PyTorch, Numpy, Pandas, Matplotlib, SciKit-Learn, Librosa, HuggingFace, NLTK, OpenCV
Machine/Deep Learning Algorithms: Logistic Regression, Decision Tree, Clustering, KNN, Random Forest, CNN, GAN, LSTM, Transformer
Algorithmic Proficiency: Multi-Modal Fusion, Object Detection, Image Classification, Semantic Segmentation, Time-Series Analysis, Supervised Learning
Hardware Proficiency: Raspberry Pi, Jetson Nano, Jetson Xavier, Google Coral Dev Board

Research Interest:

• ML/DL Model Development • Deep Model Compression for Edge Deployment • AI/ML Privacy and Security • Federated Learning.

Work Experience

Center for Real-time Distributed Sensing and Autonomy, UMBC — *Research Assistant* August 2022 - Present

- **AI on the Edge:** Multi-modal fusion (image and audio) in deep learning for image classification, object detection and AI model deployment on edge. Employed varying model compression techniques and deployed compressed multimodal DNN models across a range of resource-constrained edge devices.
- **Audio Synthesis and Security Risks:** Demonstrated the vulnerability of audio recognition systems by introducing an innovative technique capable of extracting the input vector (MFCC or Mel-spectrogram) from gradients and eventually converting it back into audio waveform. Supported by the US Army Research Lab.
- **Object Detection Model Development:** Developed camouflage object detection model based on YOLOv5 by leveraging advanced image processing and custom data augmentation strategies to train the model, in the context of battlefield applications.
- **Voice and Gesture Controlled Autonomous Robot Navigation:** Implemented user's voice command and hand gesture controlled Spot Robot navigation. Utilized finger touch and imaginary steering wheel as gesture to control the robot movement.
- **MM-Wave Radar to Detect Moving Objects:** Explored AWR1642 BOOST mmWave radar technology to detect the moving object in completely obfuscated area from a distance of 30 meter, in the context of battlefield applications, contributing to advancements for the US Army.

Privacy Preserving Machine Learning Lab — *Graduate Research Assistant* January 2021 - July 2022

- **Malicious Influences in ML Models:** Addressed malicious influence, backdoor insertion and bias introduction to DL models on computer vision and audio domain caused by targeted data poisoning attacks. Finally, developed a generalized mitigation strategy capable of defending such attacks.
- **Gradient Inversion Attacks in AI/ML:** Gradient inversion attacks reconstruct the training samples from gradients. Developed mixed precision quantization and dequantization enabled solution to defend against attacks across image, audio, and text domains and it outperforms the state-of-the art defense mechanisms.
- **Audio-Visual (AV) Multi-modal Model Development:** Developed a multi-modal deep model for object classification using both visuals (image) and audio data, with federated learning approach to avoid central data collection. Also ensured robust classification capabilities even when one modality is absent or erroneous.

UMBC — *Graduate Assistant* January 2020 - December 2020

- **Causality in GAN for Counterfactual Image Generation:** Generate counterfactual images utilizing Causal GAN by controlling noise variables and consider the texture of the object, shape of the object, background as the causation image generation process.

Ctrends Software and Services Ltd — *Data Analyst* August 2018 - September 2019

- Utilized statistical techniques to identify trends, forecast outcomes and provide actionable insights. Designed and maintained dashboards and reports to enable data-driven decision-making.

First Authored Relevant Publications

- Mixed Quantization Enabled Federated Learning to Tackle Gradient Inversion Attacks
  Venue: In Proceedings with IEEE/CVF Conf. on Computer Vision and Pattern Recognition (CVPR) 2023.
- Revealing Security Risks in Audio Recognition Systems via Gradient Inversion Attacks
  Venue: IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2024
- Secured Federated Training: Detecting Compromised Nodes and Identifying the Type of Attacks
  Venue: 21st IEEE International Conference on Machine Learning and Applications (ICMLA), 2022.
- Towards Developing Data Security Aware Federated Learning for Multimodal Contested Environment. 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. 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
  Venue: 2023 57th Annual Conference on Information Sciences and Systems (CISS), 2023.
- ARIS: A Real-Time Edge Computed Accident Risk Inference System
  Venue: In 2021 IEEE International Conference on Smart Computing, IEEE Computer Society.
- TinyM2Net: A Flexible System Algorithm Co-designed Multimodal Learning for Tiny Devices
  Venue: TinyML Research Symposium 2022.

Last Updated: February 14, 2024