

Nuzaer Omar

-  nom8m@umsystem.edu, nuzaeromar97@gmail.com
-  <https://github.com/nuzaeromar>
-  <https://scholar.google.com/citations?hl=en&user=Cq3gfl4AAAAJ>
-  <https://www.linkedin.com/in/nuzaer-omar-83b5961ab/>

Research Interests

Adversarial Attacks & Defenses in LLMs, Unsupervised Learning in LLMs, Robust and Reliable LLMs, Black-Box and Zero-Access LLM Security, Context-Aware & Phonetic Perturbations in LLM, Signal Processing

Education

- | | |
|--------------------------------|--|
| Aug 2022 - Jul 2027 (expected) |  PhD, Computer Science Department
Missouri University of Science & Technology,
Supervisor: Dr. Sanjay Madria, Result: <i>CGPA 4.00 out of 4.00, 63 credits</i> |
| 2016 – 2021 |  BSc., Electrical & Electronic Engineering Department
Chittagong University of Engineering & Technology.
Result: <i>CGPA 3.69 out of 4.00</i> |

Employment History

- | | |
|----------------|--|
| 2022 - current |  Graduate Research Assistant , Wireless to Cloud Computing Lab, Missouri University of Science & Technology, |
| 2021 - 2022 |  Lecturer , Port City International University, Bangladesh. |

Research & Technical Skills

- | | |
|---------------------------|--|
| Programming |  Python, MATLAB, C/C++, R, Verilog, Assembly(x86) |
| Tools & Frameworks |  Pytorch, Tensorflow, HuggingFace, Scikit-learn, Openattack, Pandas, OpenCV, spaCy, NLTK, Ollama, vLLM |
| Databases |  SQL, MySQL, MongoDB, Redis |
| Softwares/ Research Tools |  LaTeX, Overleaf, Git, Docker, Slurm, GNS3, Proteus, Cadence Virtuoso, Pspice |
| Machine Learning |  CNNs, Autoencoders/VAEs, Contrastive Learning, Representation Learning, YOLOv5/8, Clustering |
| NLP/LLMs |  Transformer Models (BERT, T5, GPT, BART, LLaMA), Adversarial Attacks & Defenses, Prompt Engineering, Decoding Strategies, Semantic Similarity (SBERT), Text Generation, Topic Modeling, Phonetic & Lexical Perturbations |
| Optimization & Modeling |  Loss Design (Contrastive, Reconstruction, Triplet, and KL), Hyperparameter Tuning, Model Calibration |

Research Publications

Journal Articles

- 1 Nuzaer Omar, M. U., M. Dey. (2021). Temporal Feature-Based Classification into Myocardial Infarction and other CVDS Merging CNN and Bi-LSTM from ECG signal. *IEEE Sensors Journal*, 21, 21688–21695.
 doi:10.1109/JSEN.2021.3079241

Conference Proceedings

- 1 Nuzaer Omar, S. M., Ademola Adesokan. (2025). Leveraging Pre-Trained Language Models for Realistic Adversarial Attacks. In *2025 ieee international conference on big data*.
- 2 Nuzaer Omar, M. U., M. Dey. (2020). Detection of Myocardial Infarction from ECG Signal Through Combining CNN and Bi-LSTM. In *2020 11th international conference on electrical and computer engineering (ICECE)*.
 doi:10.1109/ICECE51571.2020.9393090

Research Experience

■ Modular Black-Box Adversarial Attack Framework:

- Designed a real-time, training-free adversarial text attack system integrating MLM-based perturbations, semantic similarity filters, topic-guided insertions, and phonetic perturbation modules.
- Improved black-box attack success by up to 15% on tested datasets while maintaining semantic similarity above 80%.

■ Unsupervised Re-labeling & Robustness Enhancement Framework:

- Built an unsupervised pipeline combining Sim-Text keyword attribution, Seq2Seq autoencoding, unsupervised contrastive representation learning, and KL-divergence clustering.
- Corrected mislabeled neutral samples, boosting F1 by 10% and reducing adversarial attack success by 14% across multiple LLM classifiers.

■ Feedback-Optimized Black-Box LLM Attacker:

- Developed an adaptive black-box adversarial generator integrating tentative substitutions, PLL-ranked topic-guided replacements, and phonetic perturbations with unified scoring.
- Implemented a feedback loop that iteratively refines candidates to maximize attack success while maintaining perplexity and semantic similarity constraints.

■ Feature-Driven DL Framework for Myocardial Infarction Detection:

- Developed a multi-class MI detection framework using 21 temporal ECG features from fiducial-point extraction. This mitigated redundancy and class imbalance, achieving AUC = 99.25% and F1 = 98.86%, outperforming waveform-based baselines.
- Proposed novel temporal feature extraction algorithms for robust temporal feature extraction to ensure reliable and clinically meaningful detection under imbalanced conditions.

Relevant Graduate Courses

Advanced Topics in Artificial Intelligence | Clustering Algorithms | Machine Learning in Computer Vision | Analysis of Algorithms | Regression Analysis | Network Performance Analysis | Applied Social Network Analysis.

Project Highlights

- **Chess:** Implemented a chess program from scratch with single and two-player modes using optimized search and data structures for fast move generation.
- **NN:** Built a from-scratch binary classifier implementing custom initialization, loss/gradient calculations, and gradient-descent training.
- Developed a YOLOv5-based object detection pipeline on the FLIR thermal dataset, improving robustness in limited visibility environments.
- Developed a semantic segmentation model on the CARLA simulator dataset for pixel-level road scene parsing in autonomous driving.

Awards and Mentorship

2022 - 2026

■ Kummer Innovation and Entrepreneurship Doctoral Fellows Program

Missouri University of Science & Technology.

2025

■ NSF Local I-CORPS, Great Lakes Region

2022

Mentored a student team at PCIU that achieved a Top-20 placement in the national "Mujib 100 Idea Contest."

■ Reviewer in conferences like ICDM 2025, IEEE Big Data 2024-2025, ECML 2025, etc.