Rameen Mahmood

rameen.mahmood@nyu.edu

Summary

Ph.D. candidate in Electrical and Computer Engineering at New York University (Tandon), advised by Professor Danny Huang. My research bridges **machine learning** and **computer networks**, developing LLM-based methods for IoT device identification, behavioral inference, anomaly detection, and health monitoring. Experienced in fine-tuning and deploying foundation models end-to-end—from model training to production deployment—with additional expertise in LLM jailbreaking and prompt engineering.

Education

- **New York University, Tandon School of Engineering** — Brooklyn, NY
  Ph.D. in Electrical & Computer Engineering — *CGPA: 4.00* — *Sept. 2023 – May 2027 (expected)*
- **New York University Abu Dhabi** — Abu Dhabi, UAE
  B.Sc. in Electrical Engineering (Honors) — *Sept. 2019 – May 2023*

Research Experience

- **Graduate Research Assistant** — Sept. 2023 – Present
  mLab, NYU Tandon School of Engineering — *Brooklyn, NY*
  - **Device Identification (in research collaboration with Google)**: Built and deployed a fine-tuned **LLaMA 3.1 8B** model for real-time IoT device attribution and behavior inference from encrypted network metadata. Trained on 216K smart-home flows across 2015 vendors using **QLoRA + curriculum learning** (98.25% Top-1, 90.73% macro accuracy). Productionized on IoT Inspector via **FastAPI + Docker + Tailscale** for secure, low-latency inference.
  - **RouterSense**: Developed a passive ML system that infers sleep/wake and social behavior patterns from encrypted home network traffic. Collaborated with clinicians at Harvard, OHSU, and Northwestern; validated in a pilot with older adults for non-intrusive cognitive health monitoring.
  - **Behavioral Modeling for Blind and Low-Vision Users**: Built a machine learning pipeline to infer assistive app usage (e.g., BeMyEyes, Seeing AI) from encrypted traffic, achieving 98.8% (iOS) and 98.0% (Android) accuracy. Enabled large-scale accessibility audits for visually impaired users.
- **Research Intern** — Jan. 2023 – Aug. 2023
  Clinical AI Lab, NYU Abu Dhabi — *Abu Dhabi, UAE*
  - **Embryo Viability Modeling**: Trained **Vision Transformer, ResNet-LSTM, and 3D ResNet** on 14,776 embryo time-lapse sequences—the largest ART dataset to date—achieving >5% improvement over clinical baselines in blastocyst prediction.
  - **Automated Imaging Pipeline**: Built a deep learning system for ploidy prediction and embryo quality control; achieved 100% well detection accuracy, automating time-lapse video labeling and reducing manual annotation time for embryologists.
- **Undergraduate Research Intern** — Jun. 2022 – Aug. 2022
  NYU Tandon Summer Research Program — *Brooklyn, NY*
  - **Symmetry-Driven CNNs**: Enhanced model interpretability and robustness by embedding anti-symmetry and time-reversal invariance in CNN design, improving performance under temporal noise.

Selected Publications

- **R. Mahmood**, T. Ahmed, S. T. Peddinti, D. Y. Huang. "Large Language Models for Real-World IoT Device Identification." *arXiv preprint* arXiv:2510.13817, 2025. DOI
- **R. Mahmood**, D. Hu, A. David, Z. Beattie, J. Kaye, N. Alshurafa, L. Haux, J. Hester, A. Kiselica, S. Liu, C. Qiu, C.-Y. Wu, D. Y. Huang. "Digital Phenotyping via Passive Network Traffic Monitoring: Feasibility and Acceptability in University Students." *JMIR*, 2025. DOI
- D. Hu, **R. Mahmood**, A. David, D. Y. Huang. "Network Traffic as a Scalable Ethnographic Lens for Understanding University Students' AI Tool Practices." *arXiv preprint* arXiv:2510.09763, 2025. DOI

- **R. Mahmood**, D. Y. Huang. "RouterSense: Passive, In-Home Health Monitoring for Older Adults." *AAAI Symposium on AI for Aging in Place*, 2024. PDF
- **R. Mahmood**, D. Y. Huang. "Your Router as Fitbit: Health Monitoring with Network Traffic." *IEEE EMBS Body Sensor Networks*, 2024. PDF

Academic Highlights

- **Coursework**: Deep Learning, Machine Learning for Healthcare, ML for Network Traffic, Network Security, ML for Cybersecurity, Probability, Linear Algebra, Operating Systems
- **Teaching**: Teaching Assistant – Machine Learning, Digital Logic, Electronics, Circuits, Signals and Systems
- **Awards**: Finalist – Rhodes Scholarship (Pakistan), David and Cecilia M. Chang Leadership Award

Technical Skills

- **Languages**: Python, C/C++, SQL, Bash, JavaScript, MATLAB, Verilog
- **ML & LLMs**: PyTorch, Transformers, QLoRA, PEFT, DeepSpeed, Lightning, bitsandbytes, TensorFlow, Scikit-learn, HuggingFace Hub, LoRA, mixed-precision training, model quantization, distributed training (DDP)
- **Network Analysis**: Wireshark, nPrint, NetML, Scapy, Tshark
- **Developer Tools & Infra**: Git, Docker, FastAPI, GCP, Weights & Biases (W&B), RESTful APIs, MongoDB, DuckDB, Jupyter