MOHOSHIN ARA TAHERA

tashfinionta@gmail.com | +1 (337) 909-8795 | LinkedIn | GitHub | Google Scholar

RESEARCH INTERESTS

Federated Learning, Privacy-Preserving Machine Learning, Trustworthy AI for Healthcare, Multimodal Medical AI, Demographic Fairness in Clinical AI Systems

EDUCATION

University of Louisiana at Lafayette Aug 2024 – May 2026 (expected)
Master of Science in Computer Science | GPA: 3.75 / 4.0

- Advisor: Dr. Shuvalaxmi Dass, AI CyberSafe Innovations Lab
- Research: Federated Learning, Privacy-Preserving ML, Moving Target Defense, Trustworthy AI

Khulna University, Bangladesh 2014 – 2018
Bachelor of Science in Computer Science and Engineering

- Thesis: Image Steganography Using Genetic Algorithms

PUBLICATIONS & MANUSCRIPTS

[1] *"SoK: Privacy-Preserving Federated Learning for Large Language Models in Healthcare."*
Collaborative Lab Research | **Accepted**, **IEEE International Conference on Cybersecurity and Resilience, 2026.** **[First Author]**

[2] *"SoK: Privacy-Preservation of Large Language Models in Healthcare."*
Collaborative Lab Research | Manuscript in revision (completed two rounds of review at a top-tier security venue). **[First Author]**

[3] *"BlockSecRT-DETR: Secure and Efficient Federated Transformers for Real Time Object Detection in ITS."*
Collaborative Lab Research | **Accepted**, **IEEE 100th Vehicular Technology Conference, 2026.** **[First Author]**

[4] *"MTD-Playground: An Attacker-Aware Evaluation Framework for Network Moving Target Defense."*
Collaborative Lab Research | Manuscript in preparation. **[Second Author]**

[5] *"Federated Multimodal Bottleneck Transformer for Privacy-Preserving Ophthalmic Disease Detection."*
Collaborative Lab Research | Manuscript in preparation. **[First Author]**

ACADEMIC RESEARCH EXPERIENCE

Graduate Research Assistant — AI CyberSafe Innovations Lab Feb 2025 – Present
University of Louisiana at Lafayette

Federated Multimodal Bottleneck Transformer for Ophthalmic Disease Detection (Ongoing)

- Designing FedMBT: a federated multimodal learning framework for age-related macular degeneration (AMD) detection across hospitals with heterogeneous imaging equipment (3D OCT volumes and 2D SLO fundus photography) without sharing patient data.
- Addressing the challenge of training across sites with asymmetric modality availability, where some hospitals operate OCT scanners, others only fundus cameras, and a minority possess both.
- Evaluating on Harvard-FairVision30k (∼30K patients, two imaging modalities) across simulated hospital configurations with comprehensive demographic fairness analysis (race, sex, ethnicity subgroups).
- Deploying end-to-end distributed training pipeline on the LONI HPC cluster (SLURM, PyTorch, CUDA) with custom data-loading for large-scale retinal imaging experiments.

BlockSecRT-DETR: Secure and Efficient Federated Transformers for Real Time Object Detection in ITS (Accepted — IEEE VTC 2026)

- Engineered a federated Vision Transformer pipeline for multi-client object detection on the KITTI dataset with latency-aware adaptive token selection.
- Designed a secure multi-client evaluation protocol isolating per-client gradient updates under non-IID traffic-scene distributions.
- Achieved 89.2% mAP@0.5 with 47.8% encoder FLOP reduction and 17.2% inference latency improvement on the

KITTI benchmark under missing-class non-IID federation across clients.

Trustworthy AI: Privacy-Preserving LLMs & Federated Learning in Healthcare

- Authored two SoK papers: one on privacy threats for FL-based LLMs in clinical settings, and one on the broader LLM privacy-preservation pipeline.
- Investigating trade-offs between differential privacy guarantees and model utility with reproducible experimental frameworks.

MTD-Playground: Attacker-Aware Network MTD Evaluation Framework (In Preparation)

- Designed an enterprise-style SDN testbed (Containernet, Open vSwitch, ONOS) supporting game-theoretic, AI/ML-driven, and SDN-based MTD strategies under multi-stage attack campaigns.
- Demonstrated dynamic path randomization reduces attack success rate from 92% to 18% while maintaining acceptable latency and throughput.

Graduate Teaching Assistant – Software Methodology Aug 2024 – Feb 2025
University of Louisiana at Lafayette

- Mentored 40+ undergraduates in software engineering projects, code review, debugging, and technical documentation.

PROFESSIONAL INDUSTRY EXPERIENCE

BI Developer & Data Engineer — Grameenphone (Telenor Group) Feb 2020 – Aug 2024
Dhaka, Bangladesh | 80M+ subscribers | 4.5 years

- Engineered distributed data pipelines on Oracle Exadata, Hadoop, and Spark for ML feature engineering over 80M+ subscriber records, infrastructure experience directly transferable to scaling federated learning systems.
- Architected predictive analytics for customer churn and retailer stockout forecasting; reduced reporting overhead by 57% through pipeline automation (SQL, Qlik Sense).

Software Engineer — Shiram System Solutions May 2018 – Feb 2020
Khulna, Bangladesh

- Developed enterprise web applications (Laravel/PHP) for commercial and government clients.

SELECTED ACADEMIC PROJECTS

Privacy-Preserving Federated Vision Transformers for Pneumonia Detection
Federated Learning · Vision Transformers · Differential Privacy · Medical Imaging

- Proposed a federated ViT framework for chest X-ray pneumonia detection under non-IID distributions; designed experiments quantifying privacy–utility trade-offs across differential privacy budgets.

Glaucoma Detection Using Clinical Notes
NLP · Deep Learning · Healthcare

- Benchmarked LSTM, 1D-CNN, and Transformer architectures for glaucoma detection from unstructured clinical text with ablation studies on attention mechanisms.

Image Steganography Using Genetic Algorithms
Undergraduate Thesis · Evolutionary Computation · Information Security

- Engineered a GA-based steganographic system optimizing pixel selection and bit-embedding via fitness functions balancing payload capacity and PSNR.

TECHNICAL SKILLS

Languages: Python, Java, C/C++, SQL, Bash, PHP, JavaScript, Swift
ML & AI: PyTorch, TensorFlow, Scikit-learn, Hugging Face Transformers, Federated Learning (Flower/PySyft), Deep RL
Networking & Security: SDN (ONOS, OpenFlow), Open vSwitch, Mininet/Containernet, Nmap, Wireshark
Distributed Systems: Hadoop, Spark, Oracle Exadata, AWS, Docker, Qlik Sense, SLURM/HPC (LONI), Data Streaming

Tools: Git, Linux, Flask, Laravel, React Native, ONNX, LaTeX

AWARDS & CERTIFICATIONS

- Winner, Intra-University Programming Contest — Khulna University (2017)
- Recognition for ML-driven predictive analytics innovation — Grameenphone (2022, 2023)
- Qlik Sense Data Architect Certification | Data Streaming Nanodegree (Udacity) | Agile PM Certification