Md Zarif Hossain

zarifh493@gmail.com | +1(618)528-5595

LinkedIn | Github | Google Scholar

Carbondale, Illinois - 62901, USA

Objective

Doctoral Fellow specializing in Machine Learning, with a research focus on building robust and secure AI systems. My expertise spans Generative AI, Large Language Models (LLMs), Vision-Language Models (VLMs), and Federated Learning. I am dedicated to advancing methods that enhance the reliability, safety, and trustworthiness of AI in real-world environments. With a strong foundation in both theoretical and applied research, I aim to develop scalable, efficient, and resilient AI solutions that address industry-critical challengesparticularly those involving adversarial threats, data privacy, and model robustness. Eager to contribute to impactful projects, I am passionate about transforming cutting-edge research into practical tools that drive business innovation and system-level security.

Employment Experience

- **Advanced Research Intern** — Summer 2025
  AT&T, Bedminster, NJ
- **Graduate Research Assistant, SPEED Lab** — January 2023 - Present
  Southern Illinois University, Carbondale
- **Lecturer** — July 2022 - December 2022
  Shanto-Mariam University of Creative Technology
- **Fullstack Software developer** — July 2021 - February 2022
  Sari LLC Square, WA, USA
- **Software developer intern** — February 2021 - May 2021
  Brain Station 23 Dhaka, Bangladesh

Education

- **Ph.D. Fellow in Computer Science** — 2023 - Present
  School of Computing, Southern Illinois University, Carbondale
  GPA: 3.958 out of 4.00
- **Bachelor of Science in Software Engineering** — 2018 - 2022
  Department of Computer Science and Engineering, Islamic University of Technology, Gazipur
  CGPA: 3.79 out of 4.00

Research Interests

- **Generative AI** (Large-Language Models, Large Vision-Language Models, Generative Adversarial Networks (GAN), Deep Convolutional GAN)
- **Robust and Secure AI** (Adversarial attack and Robust defense mechanisms, Adversarial training, Secure architectures for autonomous vehicles, Cybersecurity in LLMs and VLMs)
- **Scalable AI** (Federated Learning, Computer Vision, ML, Multi-modality, Deep Learning)
- **Interdependent Networks** (Connected autonomous vehicles, Critical Infrastructure Resilience, Network Dynamics and Behavior)

Highlights

- Awarded the prestigious **SIU Doctoral Fellowship** as the sole recipient from the Computer Science department, recognizing academic excellence and research potential.
- **Published 14+ research papers** in peer-reviewed venues, including Q1 journals and A* conferences such as CVPR.
- **Contributed to a successful NSF CRII research proposal** on secure and distributed AI systems, supporting federally funded research initiatives.
- Contributed to and actively involved in **NSF and DHS-funded** research projects, with multiple publications in top-tier AI conferences such as CVPR and BigData..
- **Mentored 10+ graduate and undergraduate students**; several received research awards and published research papers at top tier venues.
- Delivered research talks at top IEEE conferences including IEEE BigData and ICMLA.
- Served as **General Secretary** of the Bangladeshi Student Association at SIU; led initiatives that earned the **Best Registered Student Organizations (RSO) Award** (2024).
- Collaborated with **academic research labs** and **industrial partners** on cutting-edge research in Generative AI and Federated Learning.
- Experienced in **full-stack software development** with a strong track record of deploying real-world web and mobile applications.

Publications

- **MZ. Hossain**, and Ahmed Imteaj. "SLADE: Shielding against Dual Exploits in Large Vision-Language Models." In IEEE/CVF Conference on Computer Vision and Pattern Recognition 2025. **(Ranked #1 CS Conference, 22.1% Acceptance Rate)**
- Moore, E., Imteaj, A., **MZ. Hossain**, Rezapour, S., & Amini, M. H. (2025). Blockchain-Empowered Cyber-Secure Federated Learning for Trustworthy Edge Computing. IEEE Transactions on Artificial Intelligence. **(Q1 Journal)**
- **MZ. Hossain**, & Imteaj, A. Securing vision-language models with a robust encoder against jailbreak and adversarial attacks. In 2024 IEEE International Conference on Big Data (BigData) (pp. 6250-6259). IEEE.
- Awal Ahmed Fime, **MZ. Hossain**, Saika Zaman, Abdur R. Shahid, Ahmed Imteaj. "Towards Trustworthy Autonomous Vehicles with Vision-Language Models Under Targeted and Untargeted Adversarial Attacks". In IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshop 2025.
- Awal Ahmed Fime, **MZ. Hossain**, Saika Zaman, Abdur R. Shahid, Ahmed Imteaj. Benchmarking Large Language Models for Resource-Efficient Medical AI at the Edge. AAAI 2025 Spring Symposium.
- Imteaj, A., **MZ. Hossain**, Zaman, S., & Shahid, A. R. (2024). TriplePlay: Enhancing Federated Learning with CLIP for Non-IID Data and Resource Efficiency. In 23rd International Conference on Machine Learning and Applications (ICMLA).
- **MZ. Hossain**, and Ahmed Imteaj. "Sim-CLIP: Unsupervised Siamese Adversarial Fine-Tuning for Robust and Semantically-Rich Vision-Language Models." arXiv preprint arXiv:2407.14971 (2024). **(Under Review in IEEE Transactions on Big Data)**
- **MZ. Hossain**, Ahmed Imteaj, and Abdur R. Shahid. "Flamingo: Adaptive and resilient federated meta-learning against adversarial attacks." 2024 IEEE 44th International Conference

on Distributed Computing Systems Workshops (ICDCSW). IEEE, 2024.

- **MZ. Hossain**, Jockusch, O., Imteaj, A., & Shahid, A. R. (2024, April). Generative AI-based Land Cover Classification via Federated Learning CNNs: Sustainable Insights from UAV Imagery. In 2024 IEEE Conference on Technologies for Sustainability (SusTech) (pp. 356-361) (IEEE Sustech 2024).
- **MZ. Hossain**, Imteaj A, Shahid AR, Zaman S, Talukder S, MH Amini. FLID: Intrusion Attack and Defense Mechanism for Federated Learning-Empowered Connected Autonomous Vehicles. In 2023 6th IEEE Conference on Dependable and Secure Computing (IEEE DSC 2023), November 12, 2023.
- **MZ. Hossain**, A. Imteaj and Abdur R. Shahid. "Fedavo: Improving communication efficiency in federated learning with african vultures optimizer." 2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, 2024.
- Shahid AR, Imteaj A, Badsha S, **MZ. Hossain** Assessing Wearable Human Activity Recognition Systems Against Data Poisoning Attacks in Differentially-Private Federated Learning. In 2023 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 355-360, Jun 26, 2023.
- Zaman S, Talukder S, **MZ. Hossain**, Puppala SM, Imteaj A. Towards Communication-Efficient Federated Learning Through Particle Swarm Optimization and Knowledge Distillation. In2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC) 2024 Jul 2 (pp. 510-518). IEEE.
- Imteaj A, Rahman T, Zaman S, **MZ. Hossain**, Shahid AR. Enhancing Road Safety Through Cost-Effective, Real-Time Monitoring of Driver Awareness with Resource-Constrained IoT Devices. In2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC) 2024 Jul 2 (pp. 1711-1720). IEEE.
- Shahid AR, Hasan SM, Kankanamge MW, **MZ. Hossain**, Imteaj A. WatchOverGPT: A Framework for Real-Time Crime Detection and Response Using Wearable Camera and Large Language Model. In2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC) 2024 Jul 2 (pp. 2189-2194). IEEE.
- Lisa, F. T., **MZ. Hossain**, Mou, S. N., Ivan, S., & Kabir, M. H. (2022, December). Land Cover and Land Use Detection using Semi-Supervised Learning. In 25th IEEE International Conference on Computer and Information Technology (ICCIT), 2022.

Selected Projects

- **Advanced Visual Instruction Tuning for Vision-Language Models in Retinopathy Diagnostics**
  This project aims to fine-tune Vision-Language Models (VLMs) for enhanced accuracy in diagnosing retinopathy using medical imaging. By leveraging advanced visual instruction tuning, the model significantly improves its interpretative capabilities, offering precise and automated insights for medical professionals.
- **Optimized Vision-Language Models for Autonomous Driving: Enhancing Perception and Decision-Making**
  This project explores the integration of Vision-Language Models (VLMs) in autonomous driving systems to improve vehicle perception and decision-making. By combining visual data with contextual language understanding, the VLMs enhance the vehicle's ability to interpret complex driving environments, making real-time decisions for safer and more efficient navigation.
- **SkyWatch: Unveiling Criminal Activity via Keypoint Analysis with Video-Streaming of**

Drones (Aerial Perspectives)
This research delves into the realm of crime detection through a pioneering integration of drone technology and developing a novel keypoint detection algorithm. The ongoing project focuses on the acquisition of criminal activity data using drones and the application of advanced keypoint detection algorithms to decipher intricate patterns and anomalies.

- **Drone Swarming, Distributed Streaming and Learning**
  This project involves orchestrating a fleet of DJI Tello drones to operate collectively. Through distributed streaming, these drones exchange real-time data and insights. This data sharing facilitates a collaborative learning environment where each drone contributes its observations and experiences to a shared knowledge base.
- **Advancing Real-time Crime Detection through Semi-Federated Learning and UAV Surveillance**
  This project presents a Semi-Federated Learning (Semi-FL) framework for real-time crime detection using UAV surveillance. By merging centralized and federated learning, it enhances data privacy and resource efficiency. The framework employs the YOLO model for weapon detection and LSTM for pose estimation, while utilizing a dedicated dataset designed for UAV surveillance. **Accepted in IEEE ICDCS 2024 (Poster)**
- **SPEED Lab Website**
  Designed and developed the official website for SPEED Lab, providing an interactive and user-friendly platform. **https://speedlab.network**
- **Farmsnearme (MERN stack)**
  A platform designed for farmers to post and showcase their fresh produce. Users can locate and visit the farms through an integrated map, facilitating direct connections between farmers and consumers.
- **GoMushroomHunting (MERN stack)**
  Built a production-level website where users can post and share their mushroom discoveries. The platform includes an integrated map that allows users to track and explore mushroom findings in different locations.

Technical Skills

- **Programming Language**: Python, C, C++, C#, Java, JavaScript, HTML, CSS, R
- **Framework**: Pytorch, TensorFlow, OpenGL, Flask, React, React native, ASP.NET, Node.js
- **Networking Tools:** Cisco Packet Tracer, TCP/IP, DNS, VPN
- **Database**: MySQL, SQLite, Oracle, Firebase
- **Software and Tools**: Android Studio, Adobe XD, Latex, Adobe Premiere Pro , AutoCAD, R Studio, Postman, Jira, Blender, Trello, Git, Figma
- **Saas and Hosting**: Firebase, AWS, Heroku, Netlify

Honors & Awards

- **SIU Doctoral Fellowship Award**
  Awarded the prestigious Doctoral Fellowship from Southern Illinois University, Carbondale, in recognition of academic excellence and research potential. This fellowship provides support for research initiatives and professional development opportunities.
- **CVPR 2025 Travel Grant Award**
  I received the prestigious CVPR 2025 Travel Grant to attend the Conference on Computer Vision and Pattern Recognition, recognizing expertise and active participation in cutting-edge

computer vision research discussions, contributing to professional growth and research network development.

- **NSF Travel Grant Award**
  I received the prestigious NSF Travel Grant to attend the MOBIHOC 2023 Conference, recognizing expertise and active participation in cutting-edge research discussions, contributing to professional growth and research development.

Professional Service

- **Reviewer in Conferences & Workshops**
  - IEEE International Conference on Distributed Computing Systems (ICDCS 2024)
  - NeurIPS Efficient Natural Language and Speech Processing (ENLSP) Workshop
- **Reviewer in Journals**
  - IEEE Transactions on Information Forensics & Security **(Impact Factor 6.3)**
- **Grant Proposal Contribution**
  - Contributed to a successful **NSF CRII** research proposal.

Mentoship

- **Masters Thesis Mentor, SPEED Lab** Fall'23 - Present
  - **Oleksandr Jockusch.** Research Topic: Federated Meta-Learning for Emotion and Sentiment Aware Multimodal Complaint Identification. **(Published paper at IEEE SUSTECH 2024)**.
  - **Dina Famouri.** Research Topic: Human Activity Recognition with Keypoint Analysis.
  - **Revathi Gajjala.** Research Topic: Physics-Informed Neural Networks.
  - **Veerendra Reddy Ayaluri.** Research Topic: Federated Learning Testbed for Mobile Agent.
  - **Sai Sandhiptha Bayya.** Research Topic: Ensuring Fairness in Federated Learning for Healthcare Systems.
  - **Mark Sidhom.** Research Topic: Develop a Fine-tuned LLM for Healthcare.
  - **Prince Duo.** Research Topic: Hallucination Attacks and Impacts on Large-Language Models.
  - **Venkata Gnana Prakash Paruchuri.** Research Topic: Topic Modelling on Research Articles using BERT.
  - **Gireesh Nadh Mekala.** Research Topic: Road Traffic Prediction using Federated Learning.
  - **Srivatsa Tangirala.** Research Topic: Poisoning Attack in Federated Learning using GANs.
  - **Madhu Nimeshika Dasika.** Research Topic: Skin Cancer Classification using Transfer Learning.
  - **Wasimuddin Fathimullah.** Research Topic: Intrusion Detection with Federated Reinforcement Learning.
- **Undergraduate Thesis Mentor, SPEED Lab** Fall'23 - Present
  - **Nadia D Lafontant.** Research Topic: Large Vision Language Models for Healthcare Domain. **(Received Research Enriched Academic Challenge (REACH) award from SIU)**.
  - **Ian Tudor.** Research Topic: Drone Swarming, Distributed Streaming and Learning.

Research Talks

- Securing vision-language models with a robust encoder against jailbreak and adversarial attacks. - **IEEE BigData (2024)**
- TriplePlay: Enhancing Federated Learning with CLIP for Non-IID Data and Resource Efficiency. - **IEEE ICMLA (2024)**
- Flamingo: Adaptive and resilient federated meta-learning against adversarial attacks. - **IEEE ICDCSW (2024), Jersey City, NJ.**
- Fedavo: Improving communication efficiency in federated learning with african vultures optimizer.- **IEEE COMPSAC (2024)**
- FLID: Intrusion Attack and Defense Mechanism for Federated Learning-Empowered Connected Autonomous Vehicles. - **IEEE DSC (2023)**
- Assessing Wearable Human Activity Recognition Systems Against Data Poisoning Attacks in Differentially-Private Federated Learning. - **IEEE SMARTCOMP (2023), Nashville, TN.**

Outreach & Extra-Curricular Activities

- **Organizer & Session Coordinator, LLMs Nexus: Bridging Technical Innovation and Ethical Horizons Workshop:** Organized and coordinated sessions for the LLMs Nexus workshop, focusing on technical advancements in LLMs and their ethical implications. Led a hands-on session introducing the basics of Vision-Language Models (VLMs) and demonstrated how VLMs can be used in real-world applications.
- **Judge at SIU Research Poster Competition:** I had the opportunity to serve as a judge at the SIU Poster Competition, where I evaluated innovative research presentations from talented students. This role allowed me to engage with emerging ideas and provide constructive feedback.
- **Judge at SIU Student Research & Creative Activities Forum:** Evaluated student research presentations and contributed to the academic development of participants through constructive feedback.
- **Organizer of IUT 10th ICT Fest 2019:** Coordinated a significant event showcasing innovative technology projects and fostering collaboration among participants from various institutions.
- **General Secretary, Bangladesh Student Association (BSA), SIU**: As the General Secretary of, I led initiatives to foster a vibrant community for Bangladeshi students, organizing events and promoting cultural awareness. Our efforts were recognized by SIU when we won the Best Registered Student Organization (RSO) Award.

References

- **Dr. Ahmed Imteaj**
  (Incoming) Assistant Professor and I-SENSE Faculty Fellow
  Department of Electrical Engineering and Computer Science, Florida Atlantic University
  Assistant Professor, School of Computing
  Southern Illinois University Carbondale
  Director, SPEED Lab **(www.speedlab.network)**
  Email: imteaj@cs.siu.edu
- **Dr. M. Hadi Amini**
  Assistant Professor,
  Knight Foundation School of Computing and Information Sciences, Florida International University and Director, solid lab

Director and PI, ADvanced education and research for Machine learning driven critical Infrastructure REsilience (ADMIRE) Center, Supported by the U.S. DHS
Associate Director and FIU PI, National Center for Transportation Cybersecurity and Resiliency (TraCR), Supported by the U.S. DOT, Senior Member, IEEE
www.hadiamini.com
www.solidlab.network
Email: amini@cs.fiu.edu