Syed Irfan Ali Meerza

PhD. Candidate @ EECS, University of Tennessee, Knoxville

(+1) 502-494-8762 | smeerza@vols.utk.edu | irfanmee.github.io/

Education

2021–2026 Ph.D., Computer Engineering, University of Tennessee, Knoxville
Dissertation Committee: Dr. Jian Liu (chair), Dr. Jinyuan Sun, Dr. Fnu Suya and Dr. Feiyi Wang
GPA: 3.77 out of 4.0

2018–2019 M.Sc., Electrical and Electronics Engineering (**Gold Medalist**), American International University Bangladesh (AIUB)
Thesis Title: Self-Modeling and Gait Control Adaptation in Multi-Legged Robot Using Q-Learning Based Particle Swarm Optimization
GPA: 3.97 out of 4.0

2011–2015 B.Sc., Electronics and Communication Engineering, Khulna University of Engineering and Technology, Bangladesh
Thesis Title: Design and Implementation of an Adaptive Control System for a GPS-Based Autonomous Unmanned Aerial Vehicle
GPA: 3.41 out of 4.0

Research Interests

My research interests lie within the domain of **AI security and privacy defenses**, **robust and trustworthy AI**, **fairness in distributed systems**, and **Smart Healthcare/Fitness**. I design adversarial perturbation techniques to safeguard creative content being exploited by generative models, methods to mitigate demographic bias in federated learning, and develop user-configurable privacy defenses.

Research Experience

AI Security and Privacy Defenses

- **HarmonyCloak.** Build a novel method to add psychoacoustically hidden perturbations to music to make it unlearnable by music generative AI models. **(S&P/Oakland 2025)**
- **Scalable Defense Against Music Exploitation.** Developed a scalable and transferable method that can prevent music from being exploited by generative models, such as training, editing, or remixing.
- **Certifiable and Robust Watermarking for Music.** Developed certifiable and robust watermarking techniques to provide ownership validation and copyright protection for music against generative models.
- **Robust Unlearnable Images.** Developed a novel framework to create unlearnable examples that are robust to relearning strategies and more acceptable to human eyes.

Fairness in Distributed Systems

- **Enhancing local and global group fairness in FL.** Developed a client-server co-design to enhance the client-level and server-level group fairness in Federated learning scenarios. **(PPAI 2025)**
- **Fairness Exploitation Threat.** Designed a novel robust model poisoning attack to exacerbate the algorithmic bias in the Federated Learning frameworks. **(IJCAI 2024)**

Robust and Trustworthy AI

- **User-Configurable Privacy Defense.** Proposed a user-configurable Federated Learning defense to protect specified personal attributes from being extracted from the gradient. **(AsiaCCS 2023)**
- **Data Unlearning from Federation Model.** Designed a neuroscience-based framework to unlearn different shards of data, such as unlearn all the data belonging to a client, a single data instance, or unlearn a particular feature from the federation model. **(ISVLSI 2024)**

Smart Healthcare/Fitness

- **mmWave-based Respiration Monitoring.** Developed a CNN-based sequence-to-sequence network to reconstruct fine-grained respiratory waveform from coarse-grained mmWave radar signal. **(IMWUT/ UbiComp 2025)**
- **Multi-modal Running Gait Analysis.** Developed a multi-modal and multi-task running gait analysis software that can monitor the runner's cadence, foot pressure distribution, and strike pattern leveraging acoustic-IMU sensor fusion. **(IMWUT/ UbiComp 2025)**

Work Experience

Graduate Research Intern, Oak Ridge National Laboratory Jan 2025–May 2025, Oak Ridge, TN
May 2024–Aug 2024, Oak Ridge, TN

- Develop a scalable and generalizable data reconstruction attack from gradients on LLMs in the FedLLM framework.
- Develop an LLM training protocol to train a proprietary large language model on clinical notes data.
- Designed a communication-efficient FL framework to train an LLM model on heterogeneous communication-restricted clients.

Executive Engineer, Bashundhara Oil and Gas Company Ltd. Feb 2017–Nov 2019, Dhaka, Bangladesh
Assistant Engineer, R&D, Walton Hi-Tech Industries Ltd. Feb 2016–Aug 2016, Dhaka, Bangladesh

Publication

Conference

[1] Bauder, C., Wu, T., **Meerza, S.I.A.**, Fathy, A., Liu, J., "mm-RunAssist: mmWave-based Respiratory and Running Rhythm Analysis During Treadmill Workouts", Accepted at ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies **(IMWUT/Ubicomp**), Espoo, Finland, October 2025.

[2] Wu, T., Wu, Y., Poudel, B., **Meerza, S.I.A.**, Gore, R., Li, W., Gao, Z., Karats, C., Liu, J., "VibRun: Real-time Unobtrusive Gait Analysis for Treadmill Running via Footstep Vibrations", Accepted at ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies **(IMWUT/Ubicomp**), Espoo, Finland, October 2025.

[3] **Meerza, S.I.A.**, Liu, L., Zhang, J., Liu, J., ''GLocalFair: Jointly Improving Global and Local Group Fairness in Federated Learning,'' The 6th AAAI Workshop on Privacy-Preserving Artificial Intelligence **(PPAI)**, Philadelphia, USA, February 2025.

[4] **Meerza, S.I.A.**, Sun, L., Liu, J., ''HarmonyCloak: Making Music Audio Unlearnable for Generative AI,'' in Proceedings of the 46th IEEE Symposium on Security and Privacy **(IEEE S&P/Oakland)**, San Francisco, USA, May 2025. **(Acceptance Rate: 14%)**

[5] **Meerza, S.I.A.**, Liu, J., ''EAB-FL: Exacerbating Algorithmic Bias Through Model Poisoning Attacks in Federated Learning,'' in Proceedings of the 33rd International Joint Conference on Artificial Intelligence **(IJCAI)**, Jeju, South Korea, August 2024. **(Acceptance Rate: 14%)**

[6] **Meerza, S.I.A.**, Sadovnik, A., Liu, J., ''ConFUSE: Confusion-based Federated Unlearning with Salience Exploration,'' in Proceedings of the IEEE Computer Society Annual Symposium on VLSI **(ISVLSI)**, Knoxville, USA, July 2024.

[7] Cui, Y., **Meerza, S.I.A.**, Li, Z., Liu, L., Zhang, J., Liu, J., "RecUP-FL: Reconciling Utility and Privacy in Federated learning via User-configurable Privacy Defense," in Proceedings of the 18th ACM ASIA Conference on Computer and Communications Security **(AsiaCCS)**, Melbourne, Australia, July 2022. **(Acceptance Rate: 16%)**

[8] Ahamed, A., **Meerza, S.I.A.**, "Iris recognition using curvelet transform and accuracy maximization by particle swarm optimization" in Proceedings of the IEEE Western New York Image and Signal Processing Workshop **(WNYISPW)**, New York, USA, November 2022.

[9] Meerza, S.I.A., Li, Z., Liu, L., Zhang, J., Liu, J., "Fair and Privacy-Preserving Alzheimer's Disease Diagnosis Based on Spontaneous Speech Analysis via Federated Learning," in Proceedings of the 44th Annual International Conference of the IEEE Engineering in Medicine and Biology Society **(EMBC)**, Glasgow, Scotland, July 2022.

[10] **Meerza, S.I.A.**, A Affan, Mirinejad, H., Brier , M.E., Zurada, J.M., Inanc, T, ''Precise warfarin management through personalized modeling and control with limited clinical data'' in Proceedings of the 43rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society **(EMBC)**, Guadalajara, Mexico, Nov 2021.

[11] Meerza, S.I.A., **Meerza, S.I.A.**, Ahmed, A., ''Food Insecurity Through Machine Learning Lens: Identifying Vulnerable Households,'' in Proceedings of the Agricultural and Applied Economics Association **(AAEA)** and Western Agricultural Economics Association **(WAEA)** Joint Annual Meeting, Austin, Texas, August 2021.

[12] **Meerza, S.I.A.**, Islam, M., Uzzal, M.M., ''Q-Learning Based Particle Swarm Optimization Algorithm for Optimal Path Planning of Swarm of Mobile Robots,'' in Proceedings of the IEEE 1st International Conference on Advances in Science, Engineering and Robotics Technology **(ICASERT)**, Dhaka, Bangladesh, May 2019.

[13] **Meerza, S.I.A.**, Islam, M., Uzzal, M.M., "Performance Evaluation of Different Algorithms for Handwritten Isolated Bangla Character Recognition", in Proceedings of 1st International Conference on Robotics, Electrical

and Signal Processing Techniques **(ICREST)**, Dhaka, Bangladesh, January 2019.

[14] **Meerza, S.I.A.**, Islam, M., Uzzal, M.M., ‘‘Optimal Path Planning Algorithm for Swarm of Robots Using Particle Swarm Optimization Technique,’’ in Proceedings of the IEEE 3rd Conference on Information Technology, Information Systems and Electrical Engineering **(ICITISEE)**, Yogyakarta, Indonesia, November 2018.

Manuscripts

[1] **Meerza, S.I.A.**, Ozturk, O., Sadovnik, A., Liu, J., ‘‘DIffUE: Enhancing Utility-Unlearnability Trade-offs in Unlearnable Examples Against Relearning with Diffusion Autoencoders,” In review.

[2] **Meerza, S.I.A.**, Wang, F., Liu, J., ‘‘FedSpy-LLM: Towards Scalable and Generalizable Data Reconstruction Attacks from Gradients on LLMs,” In review.

[3] **Meerza, S.I.A.**, Liu, J., “MusicShield: Protection for Musicians in the Era of Generative AI,” In review.

Work in Progress

[1] Harmonizing Perception: Human vs. AI Capabilities in Identifying AI-Generated Music (with Jiawei Yu, Yichen Liu, Xi Gua and Jian Liu).

[2] MusicTrace: Certifiably Robust, General Purpose Watermarking for Traceability Through Generative Music Models (with Jian Liu).

Patents

[1]

Teaching Experience

Teaching Assistant, The University of Tennessee, Knoxville

- ECE-569 Mobile and Embedded System Security (Fall 2024)
- COSC-526 Data Mining and Analytics (Spring 2024)
- COSC-522 Machine Learning (Fall 2023)

Mentorship

- **Ph.D. Student:** Tianhao Wu, Oktay Ozturk
- **Ms Student:** Xiande Zhang
- **Undergraduate Student:** Minjae Bae, Shawn-Patr Barhorst, Maximus Nwider

Awards, Travel Grants and Fellowships

Awards

- “Gonzalez Family Outstanding Graduate Research Assistant,” in recognition of outstanding performance as research assistant in the Department of Electrical Engineering and Computer Science, UTK, 2025.
- “Honoable Mention (Team)”, MagNet Challenge, Princeton University, New Jersey, USA, 2023.

- Awarded “Chancellor’s Award” and “Vice-Chancellor’s Award” for attaining academic distinction and outstanding master’s research work, 19th Convocation, AIUB, 2020.
- Winner (Team) (Khulna Division), Digital Innovation Fair 2015, ICT division, Government of Bangladesh, 2015.
- Top 20 nomination for “Young Bangla Youth Award 2015”, ICT division, Government of Bangladesh, 2015.
- 1st Runner-up Team Project Showcasing, Esonance, Islamic University of Technology (IUT), Dhaka, Bangladesh, 2014

Grants

- NSF Non-Academic Research Internship for Graduate Students (INTERN) Supplemental Funding ($55,000), 2024.
- GSS Travel Grant UTK ($400), 2025
- PPAI Workshop Travel Grant, 6th AAAI Workshop on Privacy-Preserving Artificial Intelligence ($500), 2025
- GSS Travel Grant UTK ($1,150), 2024
- IJCAI Travel Grant, 33rd International Joint Conference on Artificial Intelligence (IJCAI) ($350), 2024
- Khulna University of Engineering and Technology Merit Scholarship, 2012-2015

Fellowships

- EERE Fellow, Department of Energy Efficiency and Renewable Energy and University of Tennessee, Knoxville ($10,000), 2022-2023.
- Tennessee’s Top 100 Fellow, University of Tennessee, Knoxville ($40,000), 2021-2025

Media Mentions

- EurekAlert, “Pitch perfect protection,” May 2025
- Knox News, “You can’t hear it, but University of Tennessee tool ’cloaks’ songs to protect music from AI,” December 2024.
- The AI Musicpreneur, “New AI tool HarmonyCloak shields musicians’ work from AI copying,” December 2024.
- UTK News, “Liu’s New Tool Makes Songs Unlearnable to Generative AI,” October 2024.
- Microsoft Network, “New tool makes songs unlearnable to generative AI,” October 2024.
- FURTURA, “Bonne nouvelle pour les droits des artistes: HarmonyCloak empoisonne les IA pour protéger la musique!,” October 2024.
- NDD.news, “Protéger sa musique des IA, c’est possible !,” October 2024.
- New Atlas, “HarmonyCloak slips silent poison into music to corrupt AI copies,” October 2024.
- TechXplore, “New tool makes songs unlearnable to generative AI,” October 2024.

- Alan Cross' Journal of Musical Things, "Someone has come up with a cloaking device to fight bogus AI music. It's pretty cool," October 2024.
- Softonic, "This app is saving musicians by poisoning the AI so it stops stealing music," October 2024.
- ProjectREYLO, "HarmonyCloak: The Silent Savior Against AI Music Theft," October 2024.
- WWWHATSNEWS, "HarmonyCloak: Protección musical contra La Ia Generativa," October 2024.
- Francetvinfo, "Musique: les artistes vont pouvoir 'empoisonner' leurs œuvres pour que les algorithmes ne puissent plus s'en inspirer," October 2024.
- The Outpost, "HarmonyCloak: A New Tool to Protect Musicians from AI Copyright Infringement," October 2024.
- Ainvergo, "HarmonyCloak: Innovative AI Solution to Safeguard Music from Unauthorized Scraping by Generative AI Platforms," October 2024.
- Tecnología, "Herramienta dificulta a la IA entrenarse con canciones," October 2024.
- Knowledge, "New tech makes songs invisible to AI, protecting artists from copycats," October 2024.
- Mischa Dohler, "Harmony Unleashed: AI's Musical Revolution Silenced," October 2024.

Skills

- **Programming:** Python, C++, Javascript, Matlab, Kotlin, HTML, CSS, Latex, Git, Linux, SQL
- **Tools & Libraries:** PyTorch, Keras, HuggingFace, OpenCV, Scikit-learn, Numpy, Scipy, Pandas, Unittest
- **Cloud Computing Platforms:** AWS, Azure

Professional Activities

Reviewer: The Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI) (2024), IEEE Transactions on Network Science and Engineering (2024), KDD (2024).