Syed Irfan Ali Meerza

PhD. Candidate @ Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville

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

Education

Aug. 2021–Exp. May. 2026 Ph.D., Computer Engineering, University of Tennessee, Knoxville, TN, USA
Advisor: Dr. Jian Liu

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

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

Research Interests

Robust and Trustworthy AI

– Federated Learning

– Machine Unlearning

– Differential Privacy

– Algorithmic

Responsible Content Governance

– Creative Content Protection

– Generative Model Auditing

– Watermarking

– Foundation Model Security

Smart Healthcare and Fitness

– Intelligent Fitness Technologies

– Multimodal Sensing

– Passive Health Tracking

– Early Disease Detection

Awards, Grants and Fellowships

Awards

- “Gonzalez Family Outstanding Graduate Research Assistant,” University of Tennessee, Knoxville, 2025.
- “Honoable Mention (Team)”, MagNet Challenge, Princeton University, New Jersey, USA, 2023.
- Received “Chancellor’s Award” and “Vice-Chancellor’s Award”, AIUB, 2020.
- Winner (Team) (Khulna Division), Digital Innovation Fair 2015, Bangladesh, 2015.
- Top 20 nomination for “Young Bangla Youth Award 2015”, Bangladesh, 2015.
- 1st Runner-up Team Project Showcasing, Esonance, 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

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
- Khulna University of Engineering and Technology Merit Scholarship, 2012-2015

Selected Media Mentions

Jul. 2025 **how to poison AI music scrapers** — killswitch@kaleidoscope (Apple Podcast)

May. 2025 **Pitch perfect protection**. *EurekAlert*.

Apr. 2025 **The Art Of Poison-Pilling Music Files**. Benn Jordan (YouTube) (**615k** Views)

Dec., 2024 **You can't hear it, but University of Tennessee tool 'cloaks' songs to protect music from AI**. *Knox News*.

Dec. 2024 **New AI tool HarmonyCloak shields musicians' work from AI copying**. *The AI Musicpreneur*.

Oct. 2024 **New Tool Makes Songs Unlearnable to Generative AI**. Featured in over 20 media outlets including *TechXplore*, *Softonic*, *Futura*, *Knowridge*, *New Atlas*, etc.

Oct. 2024 **HarmonyCloak slips silent poison into music to corrupt AI copies**. *New Atlas*.

Oct. 2024 **Someone has come up with a cloaking device to fight bogus AI music. It's pretty cool**. *Alan Cross' Journal of Musical Things*.

Oct. 2024 **HarmonyCloak: A New Tool to Protect Musicians from AI Copyright Infringement**. *The Outpost*.

Oct. 2024 **HarmonyCloak: Innovative AI Solution to Safeguard Music from Unauthorized Scraping by Generative AI Platforms**. *Ainvergo*.

Oct. 2024 **Herramienta dificulta a la IA entrenarse con canciones**. *Tecnología*.

Oct. 2024 **New tech makes songs invisible to AI, protecting artists from copycats**. *Knowledge*.

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.

Graduate Research Assistant, University of Tennessee Knoxville Aug. 2021 –Present, Knoxville, TN

- Developed methods to ensure privacy, fairness, and unlearning capabilities in distributed and federated learning systems, addressing emerging challenges in algorithmic accountability and personalized data protection.
- Designed techniques to safeguard creative digital content from misuse by generative AI models, focusing on robust watermarking, auditing, and content cloaking to uphold creator rights and data ownership.
- Advanced intelligent fitness and healthcare technologies by integrating AI with multimodal sensor data, enabling unobtrusive, real-time analysis of human activity and physiological signals for improved wellness monitoring.

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] **Meerza, S.I.A.**, Yu, J., Liu, Y., Gua, X., Liu, J., "Harmonizing Perception: Human vs. AI Capabilities in Identifying AI-Generated Music," *Submitted to the 35th Usenix Security Symposium*, **(Usenix 2026)**, Baltimore, USA, Aug. 2026. (*In review.*)

[2] **Meerza, S.I.A.**, Wang, F., Liu, J., ''FedSpy-LLM: Towards Scalable and Generalizable Data Reconstruction Attacks from Gradients on LLMs," *Submitted to the 35th Usenix Security Symposium*, **(Usenix 2026)**, Baltimore, USA, Aug. 2026. (*In review.*)

[3] **Meerza, S.I.A.**, Liu, J., "MusicTrace: Certifiably Robust, General Purpose Watermarking for Traceability Through Generative Music Models," *To be submitted to the IEEE International Conference on Acoustics, Speech, and Signal Processing*, **(ICASSP 2026)**, Barcelona, Spain, Apr. 2026. (*In preparation.*)

[4] **Meerza, S.I.A.**, Ozturk, O., Sadovnik, A., Liu, J., ''DIiffUE: Enhancing Utility-Unlearnability Trade-offs in Unlearnable Examples Against Relearning with Diffusion Autoencoders," *Submitted to the 40th Annual AAAI Conference on Artificial Intelligence*, **(AAAI 2026)**, Singapore, Jan. 2026. (*In review.*)

[5] Yu, J., **Meerza, S.I.A.**, Wu, Y, Sadovnik, A., Liu, J., ''SemPurify: Semantics-Aware Data Purification Against Backdoor Attacks," *Submitted to the 40th Annual AAAI Conference on Artificial Intelligence*, **(AAAI 2026)**, Singapore, Jan. 2026. (*In review.*)

[6] **Meerza, S.I.A.**, Liu, J., "MusicShield: Protection for Musicians in the Era of Generative AI," *Submitted to the 47th IEEE Symposium on Security and Privacy*, **(IEEE S&P/Oakland 2026)**, San Francisco, USA, May 2026. (*In review.*)

[7] C. Bauder, T. Wu, **Syed Irfan Ali Meerza**, A. Fathy, J. Liu, "mm-RunAssist: mmWave-based Respiratory and Running Rhythm Analysis During Treadmill Workouts," in *Proceedings of the ACM on Interactive, Mobile,*

Wearable and Ubiquitous Technologies, **(IMWUT/UbiComp 2025)**, Espoo, Finland, Oct. 2025.

[8] T. Wu, Y. Wu, B. Poudel, **Syed Irfan Ali Meerza**, R. Gore, W. Li, Z. Gao, C. Karats, J. Liu, “VibRun: Real-time Unobtrusive Gait Analysis for Treadmill Running via Footstep Vibrations,” in *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, **(IMWUT/UbiComp 2025)**, Espoo, Finland, Oct. 2025.

[9] **Syed Irfan Ali Meerza**, L. Liu, J. Zhang, J. Liu, “GLocalFair: Jointly Improving Global and Local Group Fairness in Federated Learning,” in *Proceedings of the 6th AAAI Workshop on Privacy-Preserving Artificial Intelligence*, **(PPAI 2025)**, Philadelphia, USA, Feb. 2025.

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

[11] **Syed Irfan Ali Meerza**, J. Liu, “EAB-FL: Exacerbating Algorithmic Bias Through Model Poisoning Attacks in Federated Learning,” in *Proceedings of the 33rd International Joint Conference on Artificial Intelligence*, **(IJCAI 2024)**, Jeju, South Korea, Aug. 2024. **(Acceptance Rate: 14%)**

[12] **Syed Irfan Ali Meerza**, A. Sadovnik, J. Liu, “ConFUSE: Confusion-based Federated Unlearning with Salience Exploration,” in *Proceedings of the IEEE Computer Society Annual Symposium on VLSI*, **(ISVLSI 2024)**, Knoxville, USA, Jul. 2024.

[13] Y. Cui, **Syed Irfan Ali Meerza**, Z. Li, L. Liu, J. Zhang, J. Liu, “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 2022)**, Melbourne, Australia, Jul. 2022. **(Acceptance Rate: 16%)**

[14] A. Ahamed, **Syed Irfan Ali Meerza**, “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 2022)**, New York, USA, Nov. 2022.

[15] **Syed Irfan Ali Meerza**, Z. Li, L. Liu, J. Zhang, J. Liu, “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 2022)**, Glasgow, Scotland, Jul. 2022.

[16] **Syed Irfan Ali Meerza**, A. Affan, H. Mirinejad, M.E. Brier, J.M. Zurada, T. Inanc, “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 2021)**, Guadalajara, Mexico, Nov. 2021.

[17] **Syed Irfan Ali Meerza**, A. Ahmed, “Food Insecurity Through Machine Learning Lens: Identifying Vulnerable Households,” in *Proceedings of the Agricultural and Applied Economics Association and Western Agricultural Economics Association Joint Annual Meeting*, **(AAEA/WAEA 2021)**, Austin, Texas, USA, Aug. 2021.

[18] **Syed Irfan Ali Meerza**, M. Islam, M.M. Uzzal, “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 2019)**, Dhaka, Bangladesh, May 2019.

[19] **Syed Irfan Ali Meerza**, M. Islam, M.M. Uzzal, "Performance Evaluation of Different Algorithms for Handwritten Isolated Bangla Character Recognition," in *Proceedings of the 1st International Conference on Robotics, Electrical and Signal Processing Techniques*, **(ICREST 2019)**, Dhaka, Bangladesh, Jan. 2019.

[20] **Syed Irfan Ali Meerza**, M. Islam, M.M. Uzzal, "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 2018)**, Yogyakarta, Indonesia, Nov. 2018.

Patents

[1] Jian Liu, Syed Irfan Ali Meerza, "HarmonyCloak: Making Music Audio Unlearnable for Generative AI," U.S. Provisional Application, April 2025.

[2] Jian Liu, Syed Irfan Ali Meerza, "MusicShield: Protection for Musicians in the Era of Generative AI," U.S. Provisional Application, April 2025.

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. Students:** Tianhao Wu, Yue Cui
- **Ms Students:** Xiande Zhang, Oktay Ozturk
- **Undergraduate Students:** Minjae Bae, Shawn-Patr Barhorst, Maximus Nwider

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, IEEE Computer Society Annual Symposium on VLSI (ISVLSI) (2024)
- Reviewer, IEEE Transactions on Network Science and Engineering (2024)
- Reviewer, ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD) (2024)
- Mentor, HackUTK student hackathon, University of Tennessee (2022–2023)

- Volunteer, IEEE Computer Society – Bangladesh Chapter (2017–2019)
- Member and Mentor, MEC Robotics Club, Khulna University of Engineering and Technology, Dhaka (2012–2015)