Huzaifa Arif

🏠 15th Street, Troy, 12180, New York, USA
📬 arifh@rpi.edu ☎ (518) 961-8482 💻 https://huzaifa-arif.github.io in LinkedIn:HuzaifaArifRpi

Third year PhD Candidate with a primary interest in Trustworthy Machine Learning in Foundation Models (Fairness, Privacy, Attack Models and Robustness) in federated setting

Experience

IBM T.J Watson Research Center **Jun 2023–Aug 2023**
AI Research Extern - Trustworthy AI
Mentors: Pin-Yu Chen, Keerthiram Murugesan, Payel Das

IBM T.J Watson Research Center **Jun 2022–Aug 2022**
AI Research Extern - Trustworthy AI
Mentor: Pin-Yu Chen

Education

Rensselaer Polytechnic Institute **Jan 2021-Ongoing**
Electrical and Computer Systems Engineering Ph.D 3.95 GPA

Lahore University of Management Sciences **Aug 2017**
Electrical Engineering B.S. 3.61 GPA
Graduated with High Merit

Publications

1. **Reprogrammable-FL: Improving Utility-Privacy Tradeoff in Federated Learning via Model Reprogramming**
   IEEE Conference on Secure and Trustworthy Machine Learning, February 2023
   Authors: **Huzaifa Arif**, Alex Gittens, Pin-Yu Chen

Preprint/UnderReview

1. **DP-Compressed VFL is secure for Model Inversion Attacks**
   Authors: **Huzaifa Arif**, Timothy Castigalia, Stacy Patterson, Alex Gittens
   (preprint available upon request)
2. **Doubly Stochastic Approach to Group Fair Federated Learning**
   (To submit at ICML 2024) Authors: **Huzaifa Arif**, Alex Gittens, Pin-Yu Chen
   (preprint available upon request)
3. **Peel the Layers and Find Yourself: Revisiting Inference-time Data Leakage for Residual Neural Networks**
   (Under Review at CVPR 2024) Authors: **Huzaifa Arif**, Alex Gittens, Keerthiram Murugesan, Payel Das, Pin-Yu Chen

Patent

Differentially Private Federated Learning using Model Reprogramming **(Submitted Feb 2023)**
(Pin-Yu Chen, Bo Wu, Zhengfang Chen, Chuang Gan, **Huzaifa Arif**)

Reviewer Experience

Reviewer for International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2023)
Reviewer for Artificial Intelligence and Statistics (AISTATS) 2023
IEEE International Workshop on Machine Learning for Signal Processing (MLSP 2023)

Skills

Pytorch,Python,C++,Tensorflow,Keras,MATLAB,SQL,Sckitlearn

Awards

Travel Support Award, IEEE Conference on Secure and Trustworthy Machine Learning
Graduated on High Merit
Graduated on Dean's Honor List