Huzaifa Arif

15th Street, Troy, 12180, NewYork, USA
arifh@rpi.edu (518) 961-8482 website GitHub:https://github.com/Huzaifa-Arif 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

Education

Rensselaer Polytechnic Institute **Troy, NY**
Electrical and Computer Systems Engineering Ph.D 3.95 GPA Jan 2021–

Coursework: Machine Learning and Optimization,Introduction to Machine Learning,Privacy Preserving Federated Learning,Distributed Machine Learning,Introduction to Deep Learning,Trustworthy Machine Learning, Stochastic Optimization, Computational Linear Algebra,Computational Optimization

Lahore University of Management Sciences **Lahore , Pakistan**
Electrical Engineering B.S. 3.61 GPA
Graduated with High Merit
Coursework: Stochastic Systems,Linear Systems Theory,Digital Signal Processing,Computer Vision,Digital Control Systems,Mobile Robotics, Computer Networks

Coursera Complete Specializations
- Reinforcement Learning Specialization — Alberta Machine Intelligence Institute
- Deep Learning Specialization — Deep Learning.ai
- SQL for Data Sciences — UC Davis

Pubications

- **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)
- **DP-Compressed VFL is secure for Model Inversion Attacks** (To submit at TMLR) (Authors: **Huzaifa Arif**, Timothy Castigalia, Stacy Patterson, Alex Gittens) (preprint available upon request)
- **Doubly Stochastic Approach to Group Fair Federated Learning** (To submit at ICML 2024) (Authors: **Huzaifa Arif**, Alex Gittens) (preprint available upon request)
- **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, Pin-Yu Chen)

Patent

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

Experience

IBM T.J Watson Research Center Yorktown Heights, NY
AI Research Extern - Trustworthy AI Jun 2023–Aug 2023
Mentor: Pin-Yu Chen,Keerthiram Murugesan,Payel Das
- In my internship I worked with my mentors to investigate model leakage in different transfer learning settings using a foundation model.
- In this research we were able to develop a gradient free attack to recover private fine tuning data from a pretrained network's outputs.
- This attack was carried out on Fully Connected DNN and Residual Networks.
- We were able to show unique relationship between pretrained weights and recovery of private finetuning data.
- Submitted to CVPR (under review).

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

- In my internship at IBM I worked with my mentor Pin-Yu Chen to investigate Model Reprogramming in Federated Environment with Differential Private Learning
- Our study showed a breakthrough 60% improvement in model utility tradeoff using Repgrommable-FL over existing baselines
- This work resulted in a paper accepted at the flagship IEEE Conference on Secure and Trustworthy Machine Learning (2023). (*Acceptance Rate 26.31 %*)
- A patent has also been filed on this work (*Under Review*)

Gittens Research Lab **Troy, NY**

Research Assistant Aug 2022–

Advisor: Dr. Alex Gittens

- We proposed a new stochastic regularizer that achieves both local and global fairness based on user defined objectives
- We propose an algorithm for communication efficient testing of statistical independence and an algorithm for federated composite optimization when both functions are nonconvex
- Our results show huge improvement over the SOTA methods.
- Work to be submitted to ICML 2024

Networked Systems Lab - RPI **Troy, NY**

Research Assistant Aug 2021–May 2022

Advisor: Dr Stacy Patterson

- Worked on problems in privacy preserving vertical federated learning with Dr Stacy Patterson.
- Newly proposed method in VFL shows a differentially private model with adversarial robustness against model inversion attacks .
- This work is to be submitted at TMLR

Rensselaer Polytechnic Institute **Troy, NY**

Teaching Assistant Aug 2021–Dec 2021

- Conducted In person lab sessions of 20 hours every week for up to 120 students.Helped students in debugging code in C.
- Worked on programming MSP-EXP432P401R Development Board and TI RSLK car and helped out students
- Grading quizzes,weekly assignments and exams
- Had a TA rating of (4/5) evaluated by 120 students

Rensselaer Polytechnic Institute **Troy, NY**

Research Assistant May 2021– Aug 2021

- Worked on problems related to distributed compression (Slepian Wolf) in functional computation with Dr Derya Malak.
- Worked on problems in distributed reinforcement learning

Rensselaer Polytechnic Institute **Troy, NY**

Teaching Assistant Jan 2021– May 2021

- Was a teaching assistant for Embedded Controls (10 hours) and Electrical Circuits (10 hours)
- For Embedded Controls,I helped out students debug code in C using TI-RSLK car.Was also involved in grading exams and quizzes
- For Electric Circuits,I helped out in grading exams,quizzes and assignments.
- Had a TA rating of 4.7/5 for Embedded Controls and 4.4/5 for Electrical Circuits

Advanced Communication Lab - Lahore University of Management Sciences (LUMS) **Lahore, Pakistan**

Research Assistant Sep 2019– Aug 2020

- Developed a Simulink model in MATLAB to compare the performance of 2 by 2 Alamouti vs DSTBC with BPSK and QPSK under Rayleigh fading.
- Implemented this model on USRP N2310 and USRP X310 for testing over the air performance in indoor environments achieving very low BER for both floating and fixed points.
- Worked on developing Digital Auto Encoders that mitigated this performance loss of DSTBC compared to STBC

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 Secure and Trustworthy Machine Learning
Graduated on High Merit
Graduated on Dean's Honor List

References

Dr Pin-Yu Chen (pin-yu.chen @ ibm.com) IBM Research Mentor
Dr Keerthiram Murugesan, (keerthiram.murugesan@ibm.com) IBM Research Mentor
Dr Alex Gittens (gittea@rpi.edu) Primary Research Advisor