Shafkat Islam

✉ islam59@purdue.edu | ☎ (347)-335-8913 | shafkat-islam-456360ba | Shafkat Islam | US Permanent Resident

Education

Doctor of Philosophy (PhD) Candidate — *Computer Science* Jan 2022 - May 2025
Purdue University, West Lafayette CGPA: 3.72/4.00
Dissertation Title: Novelty Search & Secure Computing for Robust AI in Open World
Advisor: Prof. Bharat Bhargava

Master of Science (MS) — *Computer Science & Engineering* Jan 2020 - Dec 2021
University of Nevada, Reno CGPA: 4.00/4.00

Skills

Programming Languages/Frameworks: Python, C++, OpenMP/MPI, CUDA, R
Machine Learning Tools/Libraries: PyTorch, Numpy, Pandas, Tensorflow, Matplotlib, NLTK, SciKit-Learn
Miscellaneous: Linux, Shell (Bash), Git, Amazon EC2, SQL
Soft Skills: Leadership, Adaptability, Communication, Goal-Oriented, Problem-Solving

Work Experience

Occidental Petroleum Corporation (Oxy) — *Advanced Analytics Intern* May 2024 - Aug 2024

- Developed an end-to-end self-supervised contrastive pre-training-based scalable transformer model for detecting events in multi-dimensional time series ESP signals. The model can detect ESP events with a precision value of **1.0** and a recall value of **0.82**.
- Developed a deep model for clustering abnormal peaks from the extracted features in multi-dimensional large scale time series signals.
- Collaborated with engineers to understand the physical significance of ESP signals and data labels and presented the outcome to the stakeholders.

Purdue University — *Graduate Research Assistant* Jan 2022 - Present

- Developed a novelty specification framework for analyzing the robustness of deep reinforcement learning (DRL)-based AI agents. The framework can identify **1.1-4.5**× (compared to baselines) as many novelties that adversely impact the AI agent's performance[1, 2].
- Developed a domain complexity estimation model for a distributed learning framework (e.g., federated learning) for the perception domain. The estimation model shows a correlation value of **0.81** with the distributed learning accuracy[3].
- Working on bench-marking the performance of segment anything model (v2.0) in segmenting prostrate glands in the 3D PROMISE12 dataset.
- Analyzed and compared the robustness of SMS spam detection classifiers (i.e., LSTM, RNN, DNN, and Transformer).
- Qualitatively evaluated twelve heterogeneous programming languages (i.e., OpenMP/MPI, OpenCL, CUDA, etc.) and proposed a programming framework for developing a resilient computing prototype.
- Developed a linear regression-based mathematical model to analyze the correlation between multiple features and the resiliency of heterogeneous computing platforms. Proposed adaptive monitoring and orchestration framework for enhancing resiliency in the VERSAL computing platform. The proposed resiliency framework can perform computation satisfactorily even if **two-thirds** of the compute units remain under attack[4].
- Actively contributed to DARPA SAIL-ON and Sandia heterogeneous computing project and participated in drafting grant proposals for major funding agencies, including NSF, DARPA, DOE, and Sandia, leveraging in-depth research insights and strategic planning.

University of Nevada Reno — *Graduate Research Assistant* Jan 2020 - Dec 2021

- Developed a backdoor attack for federated RL systems, which can degrade the performance of task-offloading accuracy by **50%**[5, 6, 7, 8].
- Developed feature engineering techniques to enable the generalizability of anomaly detection models across multiple data transfer networks. Achieved transfer learning accuracy of **60-90%** for unseen data transfer networks[9].

Relevant Graduate Courses

• Natural Language Processing • Data Mining • Data Intensive Computing • Optimization • Machine Learning • Pattern Recognition

Awards & Professional Activities

- Employee Merit **Recognition Award**, Purdue University, 2024.
- NAU SICCS Conference **Travel Grant** (January, 2019).
- **Featured** in NAU Alumni Newsletter 2021 for promising research accomplishments.
- **PC Member/Reviewer** in AAAI 2023 & 2024, Neurips SyntheticData4ML, ICLR Workshop, IEEE CCNC, Journal of Intelligent & Robotic Sys.

Selected Publications

[1] "A Q-learning Novelty Search Strategy for Evaluating Robustness of DRL Agents in Open-world Environments". *IEEE Intelligent Systems*, 2024.

[2] "Discovering Novelty via Transfer Learning". *Springer International Semantic Intelligence Conference*, 2022.

[3] "Domain Complexity Estimation for Distributed AI Systems in Open-World Perception Domain"(under preparation).

[4] "Detect & Adapt: A Resiliency Enhancement Mechanism for Space Computing Platforms". *10th IEEE Annual Conf. on Comp. Sc. & Comp. Intelligence*, 2023.

[5] "A Triggerless Backdoor Attack and Defense Mechanism for Intelligent Task Offloading in Multi-UAV Systems". *IEEE Internet of Things Journal*, 2023.

[6] "Context-aware fine-grained task scheduling at vehicular edges: An extreme reinforcement learning based dynamic approach". *IEEE WoWMoM*, 2021.

[7] "Differential Privacy-exploited Stealthy Model Poisoning Attacks in Federated Learning". *IEEE Intl. Conf. on Mobility, Sensing and Networking*, 2021.

[8] "Exploiting Gaussian Noise Variance for Dynamic Differential Poisoning in Federated Learning". *IEEE Transactions on Artificial Intelligence (submitted)*.

[9] "Towards Generalizable Network Anomaly Detection Models". *IEEE 46th Conference on Local Computer Networks (LCN)*, 2021.

Last Updated: September 23, 2024