

RESEARCH INTERESTS

Machine Learning | Deep Learning | Computer Vision | AI Security | Natural Language Processing

EDUCATION

State University of New York (SUNY) Binghamton Binghamton, New York
PhD in Computer Science Jan 2023–Present
CGPA: 4.0/4.0

University of California Riverside (UCR) Riverside, California
MS in Electrical Engineering Sep 2021–Dec 2022
CGPA: 3.96/4.0

Bangladesh University of Engineering and Technology (BUET) Dhaka, Bangladesh
B.Sc. in Electrical and Electronic Engineering Feb 2015–Apr 2019
Major: Communication and Signal Processing

WORK EXPERIENCE

SUNY Binghamton Binghamton, New York
Graduate Research Assistant, ML Security Lab Jan 2023–Current

- Investigated security risks in Source-Free Domain Adaptation and proposed a secure framework, ensuring successful adaptation.
- Participated in the development of DNN-Defender, safeguarding quantized DNNs against targeted bit-flip attacks.

University of California Riverside Riverside, California
Graduate Research Assistant, Nozari Lab Sep 2021–Dec 2022

- Investigated and proved the linearity of aggregate dynamics in both Biological and Artificial Neural Networks.

REVE Systems Dhaka, Bangladesh
Machine Learning Engineer Feb 2020–Aug 2021

- Worked in the AI team to develop the intelligence behind Bengali Spell and Grammar Checker software, “Shothik” ([link](#)).
- Developed algorithms for accurate detection and correction of grammatical and spelling errors.

Bangladesh University of Engineering and Technology Dhaka, Bangladesh
Research Assistant, DSP Research Lab May 2019 –Jan 2020

- Build a framework for enhancing Traffic Sign Detection in adverse weather conditions.
- Explored rapid and accurate COVID-19 detection techniques from Chest Radiography using Deep Learning.

RESEARCH EXPERIENCE

Improving Security of Source-Free Domain Adaptation (SFDA) Jan 2023–Current
Supervisor: Dr. Adnan Siraj Rakin

- Addressed security issues in SFDA against malicious source domain owners injecting backdoor in source model.
- Developed a secure SFDA scheme employing model compression, knowledge transfer, and a spectral-norm-based loss penalty to counteract backdoor attacks.

In-DRAM based DNN Defense for Adversarial Weight Attack

Jan 2023–Current

Supervisors: Dr. Adnan Siraj Rakin & Dr. Shaahin Angizi

- Introduced DNN-Defender, a DRAM-based mechanism tailored for quantized DNNs.
- Utilized in-DRAM swapping to defend against targeted bit-flip attacks without extra hardware overhead.

Linearizing Effect of Spatio-Temporal Averaging in Neural Networks

Sep 2021–Dec 2022

Supervisor: Dr. Erfan Nozari

- Validated the linearity of gradient descent dynamics in ANNs with nonlinear activations.
- Proved the linearity of aggregate activity in both static and dynamic (recurrent) neural networks.

Traffic Sign Detection & Recognition in Adverse Weather Conditions

May 2019–Jan 2020

Supervisor: Dr. Md. Kamrul Hasan

- Tackled performance decline of TSDR under real-world challenging weather conditions (CCs).
- Designed a modular framework achieving improved precision and recall for TSDR in CCs.

Non-invasive Blood Glucose Monitoring System

Nov 2018–Apr 2019

Supervisor: Dr. Celia Shahnaz

- Proposed a wearable system using sensors like PPG, GSR, and a temperature sensor for non-invasive blood glucose estimation.
- Achieved comparable results to traditional glucometers, offering a more convenient monitoring alternative.

PUBLICATIONS

1. **Sabbir Ahmed**, Abdullah Al Arafat, Mamshad Nayeem Rizvee, Rahim Hossain, Zishan Guo, Adnan Siraj Rakin, “SSDA: Secure Source-Free Domain Adaptation”, 2023 International Conference of Computer Vision (ICCV). (accepted, yet to appear)
2. **Sabbir Ahmed**, Ranyang Zhou, Shaahin Angizi, Adnan Siraj Rakin, “Deep-WRA: Exploiting the Security of Deep Neural Networks using Novel Weight Replacement Attack via Bit-Flip in Memory Address”, 45th IEEE Symposium on Security and Privacy (SP). (submitted)
3. Ranyang Zhou, **Sabbir Ahmed**, Adnan Siraj Rakin, Shaahin Angizi, “DNN-Defender: An in-DRAM Deep Neural Network Defense Mechanism for Adversarial Weight Attack”, Asia and South Pacific Design Automation Conference (ASP-DAC). (submitted)
4. **Sabbir Ahmed**, Erfan Nozari, “On the Linearizing Effect of Spatial Averaging in Large-Scale Populations of Homogeneous Nonlinear Systems”, Published in: 2022 IEEE 61st Conference on Decision and Control (CDC). (Nominated for best paper award) (Paper)
5. **Sabbir Ahmed**, Erfan Nozari, “On the Linearizing Effect of Temporal Averaging in Nonlinear Dynamical Systems”, Published in: 2023 American Control Conference (ACC). (Recommended for best paper award by reviewer) (Paper)
6. **Sabbir Ahmed**, Uday Kamal, Md. Kamrul Hasan, “DFR-TSD: A Deep Learning Based Framework for Robust Traffic Sign Detection Under Challenging Weather Conditions”, IEEE Transactions on Intelligent Transportation Systems. (Paper)
7. Tasfin Mahmud, Mehedi Hossen Limon, **Sabbir Ahmed**, Mohammad Zunaed Rafi, Borhan Ahamed, Shadman Shahriar Nitol, Md. Yeasin Mia, Rafat Emtiaz Choudhury, Adnan Sakib, Arik Subhana, Celia Shahnaz, “Non-invasive Blood Glucose Estimation Using Multi-sensor Based Portable and Wearable System”, Published in: 2019 IEEE Global Humanitarian Technology Conference (GHTC). (Paper)
8. **Sabbir Ahmed**, Moi Hoon Yap, Maxine Tan, and Md. Kamrul Hasan, “Reconet: Multi-level preprocessing of chest x-rays for covid-19 detection using convolutional neural networks”, medRxiv. (Paper)

SIGNIFICANT PROJECTS

- **Signed Adversarial Attacks on Deep Networks:**
 - Conducted a comprehensive study on sign-based adversarial attacks.
 - Evaluated the impact and robustness of deep networks against FGSM, I-FGSM, and MI-FGSM attacks. ([details](#))
- **Atari Game (Ms. Pac-Man) Enhancement:**
 - Focused on enhancing the performance of Reinforcement Learning (RL) agents in Ms. Pac-Man gameplay.
 - Incorporated advanced modifications over baseline DDQN and Dueling DDQN algorithms. ([details](#))
- **Camera Model Identification:**
 - Integrated Signal Processing techniques with Deep Learning models.
 - Designed an effective solution for detecting and identifying source camera models from images, achieving high accuracy rates. ([details](#))
- **Image Captioning:**
 - Constructed an end-to-end system using a cascading architecture of CNNs and LSTMs.
 - Aimed to generate relevant and high-quality English captions for given images. ([details](#))
- **CNC Plotter with GAN:**
 - Employed Generative Adversarial Networks (GAN) to produce facial attribute-based sketches.
 - Resulting sketches were used as inputs for the CNC plotter, showcasing GAN's potential in creative applications. ([details](#)) [[poster](#)]
- **Voice-Controlled Robot:**
 - Designed a robot capable of understanding and executing voice commands.
 - Employed advanced speech recognition algorithms to process and interpret commands. ([details](#))
- **Line Following Bot:**
 - Conceptualized and developed a robot with line-following capabilities.
 - Utilized Digital Logic Design principles to ensure precise tracking and navigation along lines. ([details](#))

SKILLS

- **Programming Languages:** Python, MATLAB, C, C++, Intel-8086 Assembly
- **Simulation & Design Tools:** PSpice, Simulink, AutoCAD, Verilog
- **Machine Learning Libraries:** PyTorch, Tensorflow, Keras, Scikit-Learn

RELEVANT GRADUATE COURSE-WORKS

Machine Learning | Deep Learning | Reinforcement Learning | Design and Analysis of Algorithm

AWARDS AND HONORS

- **Clog Loss: Advance Alzheimer's Research with Stall Catchers**, Team leader of team "*acoustic_user*" that won 6th place among 922 teams from the whole world. ([link](#))
- **Bengali Handwritten Digit Recognition Competition**, Won 5th position among 57 teams from the whole country. ([link](#))
- **Kaggle APTOS 2019 Blindness Detection**, Team leader of team "*cholo model re shikhai*" that won 38th place among 2,943 teams from the whole world. ([link](#))
- **Kaggle Human Protein Atlas Image Classification**, Member of team "*The Unseens*" that won 98th place among 2,169 teams from the whole world. ([link](#))
- **IEEE Signal Processing Cup 2019**, Member of team "*Maverick*" that won 6th place among 24 teams from the whole world. ([certificate](#))
- **Received travel grant award** for attending the *ICCV 2023* conference to be held in Paris.