Prospective Students

I am looking for highly motivated Ph.D. students to join our research group starting from **Fall 2023**. We have some exciting research projects in the following topics: Security of Artificial Intelligence (AI), Computer Vision, Deep Learning, and Exploration of Hardware (e.g., CPU/GPU/FPGA) vulnerabilities in Machine Learning applications. Required qualifications for the position:

- A **Bachelor of Science** and a **Masters of Science** degree in a relevant field (Computer Science/Electrical and Computer Engineering) (Hard Requirement).
- Excellent *programming skills* (e.g., Python, C).
- A solid understanding of the *basic concepts of mathematics* (e.g., calculus, linear algebra).
- Prior experience with deep learning frameworks, i.e., **PyTorch/TensorFlow**, would be a plus.
- A prior *publication* or demonstration of *strong writing skills* (e.g., GRE(AWA)/TOEFL score).

If you are interested, do not hesitate to contact me at arakin@binghamton.edu. I would be happy to respond if you have any other inquiries or need help clarifying any concerns that you may have. I would encourage interested ones to apply for **Fall-2023** now (rolling based deadline) and mention my name in your SOP (send your CV/Resume directly to me). The assistantship (RA/TA) will cover *a full tuition waiver, a very competitive stipend (∼ 23,000 9-months) and health insurance benefits. Additional summer stipend (∼ 6k) will depend on availability of funds.*

Research Background: In recent years, Artificial Intelligence (AI) has been deployed in real-world applications because of its superior performance in various cognitive tasks. Such a widespread deployment of AI has raised several security issues in critical applications. A recently developed threat model, namely adversarial attack, poses a potent threat to hijack the functionality of the deployed inference AI model by manipulating the input and network parameters in sensitive applications such as autonomous vehicles, robotics and health care sectors. The adversity of these attacks can cause detrimental social, physical and economic impacts. As a result, the study of the in-depth analysis of the attack threats in AI and corresponding counter defenses has become a challenging and timely mission for both the industry and academia. If you are interested in working on this exciting research problem and making AI secure for our future generation, do not hesitate to contact me with relevant inquiries. I have been working on this topic for the last four years and publishing multiple (**over 30**) high impact scientific papers in top publication venues. For Example: IEEE CVPR (# 4), IEEE ICCV (# 17), IEEE T-PAMI (# 57) and top security venues like USENIX Security/IEEE S&P. Click here for the publication list. In addition, I have experience working on AI security at Mitsubishi Electric Research Labs (MERL) in 2020 as a robust machine learning research intern. If you are passionate about **Deep Learning/AI/Machine Learning** security research, I highly encourage you to apply. Our research group is committed to high-impact research and consistently pushes state-of-the-art AI Security research boundaries. Click here for more information about our ongoing research.

About Binghamton: Binghamton University graduate program is ranked 95^{th} according to (US-NEWS 2023). In computer science our program ranks: 65^{th} (CS Ranking) & 99^{th} (USNEWS-2023). The city of Binghamton is known for its affordable living cost, excellent housing facilities and beautiful natural views. It is also located very close to the (2.5 hours drive) New York City.