



# Arka Daw

*Alvin M. Weinberg Fellow*

## **Where and when did you earn your PhD?**

I earned my PhD in computer science from Virginia Tech in December 2023.

## **What was the subject of your dissertation?**

My dissertation focused on developing uncertainty quantification techniques for machine learning models, especially focusing on scientific applications such as solving partial differential equations, and lake modeling.

## **What was your dissertation's major contribution to your field?**

My dissertation led to the development of three different methodologies for improving uncertainty quantification techniques for the emerging field of scientific knowledge-guided machine learning (KGML), where the goal is to infuse scientific knowledge with deep learning models to improve overall generalizability. First, my dissertation provided a way of explicitly enforcing physics priors such as monotonicity constraints in neural networks for meaningful uncertainty quantification. Second, it provided a more general framework for quantifying uncertainty with KGML for generic physics supervision. Finally, it studied the limitations of the commonly used physics-based loss formulation in the context of physics-informed neural networks and provided strategies to mitigate them.

## **Who is your ORNL mentor and which group and division are you working in?**

At ORNL, I am mentored by Dr. Edmon Begoli and Dr. Amir Sadovnik. Dr. Begoli is the founding director of the Center for AI Security Research (CAISER), and Dr. Sadovnik is CAISER's research lead. I am affiliated with CAISER and also work with the Emerging Cyber Systems Group in the Cyber Resilience and Intelligence Division.



## What will your fellowship research focus on?

My fellowship research will focus on understanding the underlying causes behind adversarial vulnerabilities in deep learning models, ultimately aiming to develop novel deep learning architectures and training methodologies that enhance models' robustness, reliability, and trustworthiness.

## What is your project's expected contribution to your field?

My fellowship project is expected to contribute significantly to the field by enhancing our understanding of the current limitations in AI security and risks associated with state-of-the-art deep learning models. Building on this deeper understanding, the project aims to develop innovative deep learning frameworks and training methodologies to improve robustness, reliability, and trustworthiness, thus making these models suitable for deployment in critical infrastructures.

## What are your research interests?

My research interests primarily lie in the fields of deep learning and artificial intelligence (AI). My current research focuses on developing robust and trustworthy AI systems. This includes exploring their generalizability on out-of-distribution samples and enhancing their robustness against attacks (e.g., adversarial examples and data poisoning) and their reliability in terms of risk assessment. I am also very enthusiastic about tackling interdisciplinary problems in AI for science.

## What led you to science and your specific discipline?

My journey to science and specifically to my discipline began in childhood, driven by an innate curiosity about how things work. This quest for understanding led me to pursue Electronics and Communications Engineering for my undergraduate studies. It was during these years that I became fascinated with the concept of how basic linear algebra techniques, learned in math classes, could be ingeniously combined to form neural networks, which can learn to predict complex phenomenon from data. This revelation sparked my initial curiosity and propelled my research interests in AI.

## What did you do before coming to ORNL?

I was a graduate research assistant at Virginia Tech's Knowledge-Guided Machine Learning Lab, which was led by Dr. Anuj Karpatne. I also spent two wonderful summers interning at IBM's T.J. Watson Research Center in New York and at Amazon Web Services in Seattle.

## Could you share an interesting fact or two about yourself?

In my free time, I enjoy cooking and experimenting with different cuisines. I am also an avid fan of chess and cricket, enjoying both watching the games and playing occasionally.

## What nonscience topic or activity is important to you and why?

Diversity and equal opportunity are nonscience topics that hold significant importance to me. These principles are crucial because they foster inclusive environments where everyone, irrespective of their background, has a fair chance to succeed.

