

## Nuclear Engineering Seminar

# Arvind Sundaram

*Graduate Student, Purdue School of Nuclear Engineering*

**Wednesday, March 9, 2022**

**3:30pm | PHYS 112**

**Making smart industry smarter**

### Abstract

The ongoing industrial revolution, Industry 4.0, has fundamentally altered the nature of operations and collaboration among industrial systems. Augmented by digitization, data analytics and AI, “smart” industries have popped up in various sectors such as manufacturing, energy, and healthcare, enabling cross-communication across subsystems to improve operational efficiency, robustness, and product quality. However, smart industry has an increased attack surface due to its connection to the digital world, rendering them prone to sophisticated cyberattacks that can manipulate digital information at will, capable of causing damage to physical assets (e.g. Stuxnet) while remaining undetected. This talk will be a discussion on various defense measures currently employed to defend systems and their shortcomings, and introduces a novel cybersecurity paradigm that endows smart industry with the ability to detect falsified digital information and self-heal in the face of cyberattacks. It will then evolve into a discussion on protecting/masking sensitive digital information such as nuclear data from the prying eyes of AI without actually affecting the inferential properties of the data.



Arvind Sundaram is a Ph.D. Candidate in the School of Nuclear engineering at Purdue University. He obtained his B.S.N.E at Purdue in Spring 2019, and started his graduate career in May 2019 in the field of cybersecurity for nuclear power with his advisor, Dr. Hany Abdel-Khalik. He has authored multiple publications focused on intrusion detection of sophisticated cyberattacks in industrial systems via the Covert Cognizance paradigm, and has recently co-developed a data masking methodology for sensitive industrial data while preserving its inferential properties, called the Deceptive Infusion of Data.