Title

Leveraging Machine Learning and Explainable AI for Enhanced Cybersecurity

Speaker

Sanjay K. Jha
Professor and Director of Research and Innovation at the School of Computer Science and Engineering
Lead Cybersecurity Cooperative Research Centre, UNSW

Abstract

This presentation explores the use of machine learning to improve cybersecurity. By combining machine learning with techniques that explain how models work and protect privacy, we can create stronger cybersecurity solutions. We'll look at a few specific examples: Machine learning has been used to classify network traffic for a long time. We'll discuss a new method that uses neural networks to accurately identify harmful traffic on the Tor network. To make the model's decisions clear and trustworthy, we can use techniques that explain how it works. Also, new large language models for network traffic classification raise questions about transparency. We'll discuss the risks of making wrong conclusions when these models are used with encrypted traffic. Telecommunication infrastructure is very important, and companies in this sector need to follow rules and meet obligations. We'll talk about CompliNet, a security assistant that uses large language models to help network security experts quickly find compliance information through conversations.

Biography

Sanjay K. Jha is a Professor and Director of Research and Innovation at the School of Computer Science and Engineering, University of New South Wales (UNSW), Australia, and leads UNSW in the Cybersecurity Cooperative Research Centre. With over two decades of experience in the field, he has made significant contributions to the development of robust and secure network systems. Dr. Jha's research interests span a wide range of cybersecurity topics, including artificial intelligence, generative AI, network security, and the security of mobile devices and IoT. He has published extensively in top-tier journals and conferences, and his work has been widely cited by his peers. Beyond his academic pursuits, Dr. Jha has also been actively involved in the cybersecurity industry. He has consulted for major organizations and served on the editorial boards of several leading IEEE journals. As a dedicated educator, Prof Jha has supervised 32 PhD students and has been a mentor to many postdoctoral fellows. https://www.unsw.edu.au/staff/sanjay-jha