THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

AI in Cybersecurity (for Critical Infrastructure Protection)

Tentative List of Guest Speakers

Bio-Sketch

Arupjyoti (Arup) Bhuyan

Directorate Fellow
National & Homeland Security
Idaho National Laboratory

Director
INL Wireless Security Institute

Dr. Arupjyoti (Arup) Bhuyan is the Director of the Wireless Security Institute (WSI) and a Directorate Fellow in the Idaho National Laboratory(INL). The focus of his research is on secure implementation of future generations of wireless communications with scientific exploration and engineering innovations across the fields of wireless technology, cybersecurity, and computational science. Specific goals are to lead and focus wireless security research efforts for 5G/6G and Wi-Fi 6E/7 with national impact, to secure 5G/6G spectrum sharing with distributed scheduling, and to secure cellular communication for a nationwide unmanned aerial system.

Arup is currently the primary investigator (PI) of the 5G Threat Assessment program work in INL for the Office of the Undersecretary of Defense for Research and Engineering (OUSD R&E) in the Department of Defense (DoD). He serves as a Member of the Advisory Board in Platform for Open Wireless Data-driven Experimental Research (POWDER), in the University of Utah.

Arup has extensive industry experience in wireless communications from his work before he joined INL in October 2015. He received his Ph.D. in Engineering and Applied Sciences from Yale University. He is a senior member of IEEE.

Topic Title: AI/ML for Secure Cellular Networks in the Critical Infrastructure

Abstract: 5G, the current cellular technology adopted worldwide has started transforming wireless communications. Security and resiliency improvements in 5G along with its capability to operate with unlicensed and shared spectrum without any licensed spectrum, has made its use in the critical infrastructure highly practical. In addition to deploying 5G securely, monitoring and detecting any abnormalities and attacks on these networks are a necessity for their use in the critical infrastructure. Use of AI/ML is essential to design and implement these capabilities by processing vast amounts of network data and making near real time decisions to protect these mission critical communication networks.

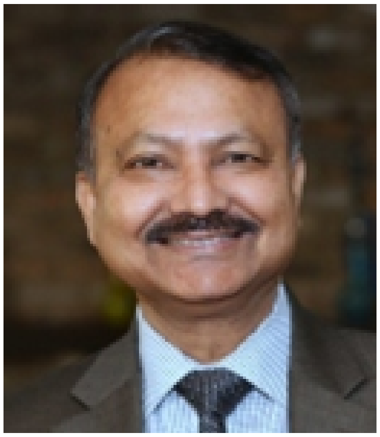
In this talk we start with the primary attack surfaces in 5G and how AI/ML can play a major role towards secure use of 5G and in the future, 6G technologies. Next, we discuss the architecture built into the 5G networks by the 3GPP specifications to support the implementation of AI/ML based solutions. The support for AI/ML implementations continues in both the Open RAN base stations and 6G, which is projected to be AI native when 3GPP starts work in the 6G for the Release 20 of its specifications. We conclude with a summary of AI/ML use to secure the current cellular networks and how it will grow in the future.

Dr. Gerry Vernon Dozier, Charles D. McCrary Eminent Chair Professor of Artificial Intelligence & Cyber Security, Department of Computer Science & Software Engineering, Auburn University

Bio-Sketch: Gerry Vernon Dozier, Ph.D.**,** is the Charles D. McCrary Eminent Chair Professor of Artificial Intelligence & Cyber Security in the Department of Computer Science & Software Engineering at Auburn University. Dr. Dozier is the director of the Adversarial Artificial Intelligence & Identity Research (A2I2R) Lab. He is currently applying his research expertise in the areas of Artificial Intelligence, Machine Learning, Adversarial Machine Learning, Behavioral Analytics, Natural Language Processing, and Evolutionary Computation to the areas of Adversarial AI, Authorship Attribution, Adversarial Authorship (Authorship Privacy), and Cyber Identity Protection & Privacy. Dr. Dozier has published over 140 conference and journal publications. He earned his Ph.D. in Computer Science from North Carolina State University. On July 24, 2019, Dr. Dozier was appointed to the Alabama Commission on Artificial Intelligence and Associated Technologies by Governor Kay Ivey.

Topic Title: Three AI/Cyber Hybrids: SecureAI, CyberAI and SecureCyberAI

Abstract: We are witnessing an exciting continuum as a result of hybridizing Artificial Intelligence and Cybersecurity! In this talk, we will briefly outline three of them: SecureAI (making AI systems more secure), CyberAI (using AI for Cybersecurity), and SecureCyberAI (making the AI used for CyberAI more secure). Additionally, we will introduce and highlight some of the ongoing AI & Cybersecurity research from AI@AU (https://eng.auburn.edu/ai-au/), Auburn University's Artificial Intelligence Initiative.



Prof. Dipankar Dasgupta, IEEE Fellow, NAI Fellow
William Hill Professor of Computer Science
Director, Center for Information Assurance (CfIA)
The University of Memphis
Homepage: www.cs.memphis.edu/~dasgupta
IA center: cfia.memphis.edu
e-mail: dasgupta@memphis.edu

Bio-sketch: Dr. Dipankar Dasgupta is a professor of Computer Science at the University of Memphis since 1997. He completed his Ph.D in 1994 on the topic of nature-inspired genetic algorithms for Search and Optimization. His research interests are broadly in Artificial Intelligence (AI); specifically, design, and development of AI-based security solutions and security of AI models. His notable works in digital immunity, negative authentication, AI-Based cloud insurance modeling, dual-filtering for secure ML and adaptive multi-factor authentication demonstrated the effective use of various AI/ML algorithms in real-world applications. His research accomplishments and achievements have appeared in Computer World Magazine, NASA's website, and in TV Channels and Newspapers.

Dr. Dasgupta has authored/edited four books, 6 patents (including 2 under submissions) and have more than 300 research publications (22,000 citations as per google scholar with H-index of 67) in book chapters, journals, and international conference proceedings. Among many awards, he was honored with the 2014 ACM-SIGEVO Impact Award for his seminal work on negative authentication, an AI-based approach. He also received five best paper awards in different international conferences and has been organizing Symposium on Computational Intelligence in Cyber Security at IEEE SSCI since 2007. Dr. Dasgupta is an IEEE Fellow, and NAI Fellow, an ACM Distinguished Speaker (2015-2020), an IEEE Distinguished Lecturer (2022-2024) and NSF-Fulbright Distinguished Scholar (CoE to Iceland 2024). He regularly serves as panelist and keynote speaker and offer tutorials in leading computer science conferences and have given more than 350 invited talks in different universities and industries.

Topic Title: Pitfalls of Generic Large Language Models (GLLMs) from reliability and security perspectives.

***Abstract*:** Generic Large Language Models (GLLMs) are continuously being released with enhanced size and capabilities, promoting the abilities of these Generative AI at the grassroots level in businesses. These tools excel in text, image, and video generation (assembling, summarizing, translating) with proper queries and prompts; moreover, various augmentation of up-to-date knowledge bases (such as RAGs), making these more efficient in providing current events. Practitioners and marketers showcase the benefits of GLLMs by demonstrating various use cases. However, the reliability of GLLMs' responses is yet questionable in certain scenarios, particularly due to issues like hallucinations, factual inaccuracies, and inappropriate or unrelated responses. Also there remain many open questions on data collection, privacy and ethical issues those need to be addressed. This talk will discuss the reliability and security aspects of GLLMs while recognizing significant benefits in a wide variety of applications. I also will provide some insides of social impacts and future directions of Generative AI applications.

Trina L. Hill, Founder & CEO of TLH Consulting Enterprises, MBA – Leadership & Business Administration, BBA – Management Information Systems

Bio-sketch: Trina L. Hill is a prominent consultant and technology leader with over 25 years of experience in technology including enhancing security measures within the energy sector. As the Founder and CEO of TLH Consulting Enterprises, she specializes in implementing cyber security solutions to protect critical energy infrastructure from cyber threats. Trina has a proven history of driving innovation and transformation implementing AI solutions in Fortune 200 companies, focusing on risk management, incident response, and organizational change.

Her dedication to addressing the cybersecurity skills gap is evident in her development of solutions for top energy companies. A sought-after speaker, coach, and business consultant, Trina is known for her engaging insights on resilience, leadership, and the importance of diversity in technology.

Trina holds a Bachelor of Business Administration in Management Information Systems and an MBA in Leadership and Business Administration, along with multiple industry certifications. Her commitment to empowering organizations and individuals ensures that the energy sector is well-equipped to navigate the complexities of cybersecurity in an increasingly digital world.

Topic Title: AI in Cybersecurity: Strengthening the Energy Sector Against Cyber Threats

Abstract: As the energy sector faces an increasing number of cyber threats, the integration of Artificial Intelligence (AI) into cybersecurity strategies has become essential for safeguarding critical infrastructure. Th is workshop will explore the innovative applications of AI in enhancing the security of energy systems, including power generation, transmission, and distribution networks. Participants will learn how AI technologies can enable real-time monitoring, anomaly detection, and predictive analytics to eff ectively identify and respond to potential threats.

The session will also address the unique challenges posed by the energy sector's aging workforce. As seasoned professionals retire, organizations risk losing valuable knowledge and expertise. We will discuss AI-driven training and mentorship programs designed to upskill younger professionals and ensure a seamless transfer of knowledge within cybersecurity teams. Attendees will leave with actionable insights and practical tools for leveraging AI to bolster their cybersecurity measures and protect the integrity of the energy sector against evolving cyber risks.

Sanjay K Madria, Curators’ Distinguished Professor, Department of Computer Science, Missouri University of Science and Technology, Rolla, MO 65409, USA

Bio-Sketch: Sanjay K Madria is a Curators’ Distinguished Professor in the Department of Computer Science at the Missouri University of Science and Technology (formerly, University of Missouri-Rolla, USA). He has published over 300 Journal and conference papers in the areas of mobile and sensor computing, big data and cloud computing, data analytics and cybersecurity. He won five IEEE best papers awards in conferences such as IEEE MDM and IEEE SRDS. He is a co-author of a book (published with his two PhD graduates) on Secure Sensor Cloud published by Morgan and Claypool in Dec. 2018. He has graduated 20 PhDs and 34 MS thesis students, with 10 current PhDs. NSF, NIST, ARL, ARO, AFRL, DOE, Boeing, CDC-NIOSH, ORNL, Honeywell, and others have funded his research projects of over $25M. He has been awarded JSPS (Japanese Society for Promotion of Science) invitational visiting scientist fellowship, and ASEE (American Society of Engineering Education) fellowship. In 2012 and in 2019, he was awarded NRC Fellowship by National Academies, US. He is ACM Distinguished Scientist and served as an ACM and IEEE Distinguished Speaker He is an IEEE Senior Member as well as IEEE Golden Core Awardee.

Topic Title: Detection of Anomalous Data and Malicious Sensors in Connected and Autonomous Vehicle Networks

Abstract: The adoption of connected and automated vehicles (CAVs) has sparked considerable interest across diverse industries, including public transportation, underground mining, and agriculture sectors. However, CAVs' reliance on sensor readings makes them vulnerable to significant threats. Manipulating these readings can compromise CAV network security, posing serious risks for malicious activities. In this talk, I will discuss a novel framework tailored to CAV networks, called CAV-AD, for distinguishing abnormal readings amidst multiple anomaly data while identifying malicious sensors. Specifically, CAV-AD comprises two main components: i) A novel CNN model architecture called optimized omni-scale CNN (O-OS-CNN), which optimally selects the time scale by generating all possible kernel sizes for input time series data; ii) An amplification block to increase the values of anomaly readings, enhancing sensitivity for detecting anomalies. Not only that, but CAV-AD integrates the proposed O-OS-CNN with a Kalman filter to instantly identify the malicious sensors. CAV-AD has been extensively trained using real-world datasets containing both instant and constant attacks, evaluating its performance in detecting intrusions from multiple anomalies, which presents a more challenging scenario. Results demonstrate that CAV-AD outperforms state-of-the-art methods, achieving an average accuracy of 98% and an average F1 score of 89%, while accurately identifying the malicious sensors.

Dr. Jungwoo Chun, MIT Cybersecurity Clinic
Lecturer of Climate, Sustainability, and Negotiation
Ph.D. in Environmental Policy and Planning
MIT Department of Urban Studies and Planning (DUSP)

Bio-Sketch: Jungwoo Chun is a lecturer at the Department of Urban Studies and Planning at MIT. He co-leads the MIT Cybersecurity Clinic and has helped launch it since 2019. The MIT Clinic (11.074/11.274) has been so successful that now there is a Consortium of University-based Cybersecurity Clinics modeled on the MIT Clinic (https://cybersecurityclinics.org/).

Topic Title: The MIT Cybersecurity Clinic: teaching, research, and public service

Abstract: Cybercriminals are locking towns, cities, and companies out of their data and demanding a ransom to restore the files. A new report suggests there were over 420 million attacks on critical infrastructure in 2023, marking a 30% increase from 2022. The MIT Cybersecurity Clinic, initiated in 2019, involves a group of MIT faculty, students, and researchers helping public agencies defend themselves against cyberattacks using an approach called Defensive Social Engineering (DSE). The MIT Clinic works with municipal or hospital IT staff and cybersecurity specialists in public agencies, especially those involved in managing critical urban infrastructure, to provide a rapid assessment of their vulnerabilities to attack. In this talk, the Clinic's co-director, Jungwoo Chun will share the Clinic's experience and reflect on their work to date.

Dr. Uttam Ghosh, Associate Professor of Cybersecurity, Founder & Director DISCS lab – Computer Science & Data Science at Meharry Medical College, Nashville, TN

Bio-Sketch: Dr. Uttam Ghosh is an Associate Professor of Cybersecurity and the Founder and Director of the NSA-funded DISCS lab in Computer Science and Data Science at Meharry Medical College in Nashville, TN. He also represents his department on the Meharry Senate and serves on the Research Advisory Council (RAC). Previously, he was an Assistant Professor of the Practice at Vanderbilt University, where he received the 2018–2019 Junior Faculty Teaching Fellow award. Dr. Ghosh earned his MS and PhD in Electrical and Electronic Engineering from the Indian Institute of Technology Kharagpur, India. He has held postdoctoral positions at the University of Illinois at Urbana-Champaign, Fordham University, and Tennessee State University. His research has received funding from organizations including NSF, NSA, DoD, DoE, NASA, South Big Data Hub, and TMCF. He has coedited and published 9 books and authored over 150 papers in prestigious international journals and conferences. Dr. Ghosh is recognized among the top two percent of cited scientists in the Stanford-Elsevier list of the world's most-cited scholars. Currently, he is working with the Coalition for Health AI (CHAI) to develop guidelines for credible, fair, and transparent health AI systems. His primary research interests include Cybersecurity, Machine Learning, IoT, and Cyber-Physical Systems. Dr. Ghosh is a Senior Member of IEEE and a member of ACM.

Topic Title: Revolutionizing Smart Healthcare: An Edge-Cloud Framework for Secure Data Sharing and Emotion Detection

Abstract: The healthcare industry is undergoing a significant digital transformation driven by IoT technologies, leading to a dramatic increase in medical data. While traditional cloud computing can effectively process this data for high-quality care, it faces challenges related to latency, data privacy, and security. Additionally, data sharing among healthcare institutions is complicated by geographical dispersion, varying ethical standards, and risks of data breaches. To address these challenges, a robust and secure framework is essential for facilitating data sharing while ensuring privacy. This talk introduces an innovative edge-cloud interplay framework designed for efficient, secure, and privacy-preserving data sharing and processing within intelligent healthcare systems. The framework leverages software-defined 5G and AI-enabled distributed edge-cloud technologies to achieve the following: (i) Integrate AI/ML at Intelligent Edge (IE) Servers: Classify healthcare data and identify potential medical conditions; (ii) Facilitate Real-Time Service Delivery: Utilize 5G slices and edge-cloud interplay for immediate service provision, crucial for latency-sensitive elderly care requiring rapid processing of complex DNN-based AI models to address emergencies like fall detection and heart attacks. (iii) Ensure Secure and Privacy-

Preserving Data Sharing: Implement blockchain and homomorphic encryption-based federated learning to safeguard health data. Additionally, this talk explores emotion detection in smart healthcare applications using a CNN-based Maximum A Posterior Estimator of Magnitude-Squared Spectrum approach. This method enhances healthcare systems' ability to monitor and respond to patients' emotional states, enriching the overall care experience.

Dr. Kul Subedi, RHCE, OSCP, Senior Security Researcher, Microsoft MSRC V&M

Bio-Sketch: "I am working in the security space to minimize the risk of assets used in information technology. I am interested in deep-diving into the components of the system and finding the gaps in designs, implementations, deployments, and operations. I have completed a PhD in Computer Science and hold security certifications: Offensive Security Certified Professional (OSCP), Software Security Practitioner - Defending C++. In addition, I hold Redhat certified engineer (RHCE) and Cisco certified network associate (CCNA) certification as well."

Topic Title: "How is the Security Landscape Changing Due to Opensource, 3P library/component, and AI-generated code?"

Abstract: "I will be presenting the impact of open-source libraries, third-party (3P) components, and AI-generated codes used in real-world production systems. I will talk about a recent backdoor in the XZ library, a service outage due to a CrowdStrike outage, and AI-generated code. I will also talk about the Microsoft Bug Bounty program (https://www.microsoft.com/en-us/msrc/bounty)."