NJIT Cybersecurity Research Center and Department of Computer Science

Securing Big Data in the Age of Artificial Intelligence

Murat Kantarcioglu
University of Texas at Dallas

Hosted by Shantanu Sharma

Date: Wednesday, November 15, 2023
Refreshments: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
Webex Link: https://njit.webex.com/njit/j.php?MTID=m00991edede3ef0606741d29fbd16a512

Abstract:

Recent cyberattacks have shown that the leakage/stealing of big data may result in enormous monetary loss and damage to organizational reputation, and increased identity theft risks for individuals. Furthermore, in the age of big data and Artificial Intelligence (AI), protecting the security and privacy of stored data is paramount for maintaining public trust, accountability and getting the full value from the collected data. Therefore, we need to address security and privacy challenges ranging from allowing access to big data to building novel AI models using the privacy sensitive data. In this talk, I provide an overview of our end-to-end solution framework that addresses these security and privacy challenges that arise in the age of AI. In addition, we will discuss our federated learning framework that is designed to be robust against poisoning attacks and when humans can work with AI to improve decision outcomes.

Bio:

Dr. Murat Kantarcioglu is an Ashbel Smith Professor in the Computer Science Department and Director of the Data Security and Privacy Lab at The University of Texas at Dallas (UTD). He received a PhD in Computer Science from Purdue University in 2005 where he received the Purdue CERIAS Diamond Award for Academic excellence. He is also a faculty associate at Harvard Data Privacy Lab and a visiting scholar at UC Berkeley RISE Labs. Dr. Kantarcioglu's research focuses on the integration of cyber security, data science and blockchains for creating technologies that can efficiently and securely process and share data.

His research has been supported by grants including from NSF, AFOSR, ARO, ONR, NSA, and NIH. He has published over 170 peer reviewed papers in top tier venues such as ACM KDD, SIGMOD, ICDM, ICDE, PVLDB, NDSS, USENIX Security and several IEEE/ACM Transactions as well as served as program co-chair for conferences such as IEEE ICDE, ACM SACMAT, IEEE Cloud, ACM CODASPY. Some of his research work has been covered by the media outlets such as the Boston Globe, ABC News, PBS/KERA, DFW Television, and has received multiple best paper awards. He is the recipient of various awards including NSF CAREER award, the AMIA (American Medical Informatics Association) 2014 Homer R Warner Award and the IEEE ISI (Intelligence and Security Informatics) 2017 Technical Achievement Award presented jointly by IEEE SMC and IEEE ITS societies for his research in data security and privacy. He is also a fellow of AAAS, and IEEE.