



Department of Computer Science

Trust in Data-Driven Systems

Shantanu Sharma

Department of Computer Science, University of California, Irvine, USA.

Hosted by Vincent Oria

DATE: Monday, May 10, 2021

TIME: 2:30 PM - 3:30 PM

LOCATION: <https://njit.webex.com/njit/j.php?MTID=mcf788021ce5d0d4800f9238e88557afd>

<https://cs.njit.edu/seminars>

Abstract: Widespread adoption of sensor data-driven approaches requires mechanisms/technologies to overcome the challenge of trust – both in the data itself and in the infrastructure that processes the data. A key building block for data-driven applications is the cloud infrastructure to store, compute, analyze, and share the data.

In the first part of the talk, I show that the existing security/privacy techniques are incapable of supporting data-driven systems, due to the high velocity of (sensor) data, a large volume of data, and the complexity of the analysis tasks over the collected (sensor) data. Addressing such concerns at scale requires significant innovations in developing new security protocols, and I describe two solutions: *Obscure* that provides string-matching-based secure and verifiable computations over the secret-shared datasets, and *Panda* that uses the concept of data sensitivity to support database operations over large volumes of data.

In the second part of the talk, I discuss privacy-related challenges at different stages of a data-driven system (such as acquisition, storage, query processing, and sharing) and present possible approaches to addressing the issues. To illustrate such challenges, I describe a real-time, privacy-preserving, and campus-wide IoT testbed, called *TIPPERS*, that I have co-developed at UC Irvine.

Bio: Shantanu Sharma is a Post-Doctoral Fellow at University of California, Irvine, USA, working in the research group of Prof. Sharad Mehrotra. He received his Ph.D. in Computer Science in 2016 from Ben-Gurion University, Israel, under the supervision of Prof. Shlomi Dolev. He obtained his Master of Technology (M.Tech.) degree in Computer Engineering from the National Institute of Technology, Kurukshetra, India, in 2011. He was awarded the gold medal for his M.Tech. degree (the gold medal recognizes the student ranked first).

His research interests include database management systems, IoT systems, and security/privacy in databases. One of his papers has received the best paper award at IEEE NCA, and one of his posters has received the distinguished poster award at ACM CODASPY. His work on secure database management systems has been

published in tier-1 databases conferences (ACM SIGMOD, VLDB, IEEE ICDE) and in several IEEE/ACM Transactions. He was the leading organizer/presenter of tutorials on advances in secure data management at IEEE ICDE 2020 and IEEE Big Data 2019. He collaborated with Prof. Jeffrey Ullman (Stanford University, USA), Prof. Nalini Venkatasubramanian (University of California, Irvine, USA), Prof. Murat Kantarcioglu (University of Texas at Dallas, USA), and Prof. Foto Afrati (National Technical University of Athens, Greece).