Computer Science

Georgia State University

The GSU CS Department Presents

Secure Computation with Privacy Preservation for Cyber Physical System Applications

Zhu Han, University of Houston

Time and Place: Thursday, January 23, 2020. 4:30 PM at Conference Room 755, 25 Park Place

Abstract: Cyber Physical System (CPS) have infiltrated into many areas such as aerospace, automobiles, chemical processing, civil infrastructure, energy, healthcare, transportation, entertainment, and consumer appliances due to their tight integration of computation and networking capabilities to monitor and control the underlying systems. Many domains of CPS such as smart metering, sensor/data aggregation, crowd sensing, traffic control etc., typically collect huge amounts of individual information for data analysis and decision making, therefore privacy is a serious concern in CPS. Most of the traditional approaches protect the privacy of individual's data by employing trusted third parties or entities for data collection and computation. An important challenge in these large-scale distributed applications is how to protect the privacy of the participants during computation and decision making, especially when such third party entities are untrusted. Considering various CPS applications involving modeling, we first discuss on utilizing applied cryptographic techniques for privacy preserving secure computation. Then we focus on the differential privacy based secure computation that guarantees individual privacy in presence of untrusted third party entities. Since confidential information must not be inappropriately released, and the use of untrusted information must not corrupt trusted computation and the utility. This talk concludes by focusing on the development of such tools for state-of-the-art applications by considering application-specific information security requirements.

Bio: Zhu Han received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 2003. Currently, he is a John and Rebecca Moores Professor in the Electrical and Computer Engineering Department as well as in the Computer Science Department at the University of Houston, Texas. He is also a Chair professor in National Chiao Tung University, ROC. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid. Dr. Han received an NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the Journal on Advances in Signal Processing in 2015, IEEE Leonard G. Abraham Prize in the field of Communications Systems (best paper award in IEEE JSAC) in 2016, and several best paper awards in IEEE conferences. Dr. Han was an IEEE Communications Society Distinguished Lecturer from 2015-2018, IEEE Fellow since 2013, and AAAS fellow since 2019 and ACM distinguished Member since 2019. Dr. Han is 1% highly cited researcher since 2017 according to Web of Science.