Other - LSU Faculty Candidate Seminar- Cyber Risk (joint Business-CCT position)

Privacy Preserving Analysis: Private Recommendation Generation and Private Information Learning

Shahriar Badsha, Cybersecurity Center, Department of Computer Science and Engineering, University of Nevada, Reno

Postdoctoral Researcher

Digital Media Center 1034
January 18, 2019 - 08:30 am

Abstract:
With the rapid development of the online social networks, various recommendation systems have been increasingly prevalent and become widely accepted by users. Usually, the recommendation system predicts the ratings for users by collecting privacy sensitive data from users. However, the users are sensitive to disclosure of personal information and, consequently, there are unavoidable privacy concerns since private information can be easily misused by malicious third parties. In order to protect against breaches of personal information, it is necessary to obfuscate user information by means of efficient encryption technique while simultaneously generating the recommendation by making true information inaccessible to service providers. The homomorphic cryptography-based techniques have the ability to perform certain operations while the data are encrypted. Also, the advantage of homomorphic based cryptography is that they are semantically secure i.e., it is computationally hard to find plaintext from the ciphertext. So, this research talk presents what are the different types of recommendation system, what are their privacy requirements and how a server can generate recommendations for users using the encrypted information without actually learning about the information, by leveraging the homomorphic properties of public key cryptography.

In this research talk, Shahriar Badsha is also going to share his current research work which is on cybersecurity information sharing and privacy preserving learning to build proactive cyberdefense.

Speaker's Bio:
Shahriar Badsha is working as a postdoctoral researcher at Cybersecurity Center, Department of Computer Science and Engineering, University of Nevada, Reno since August 2018. Shahriar obtained his PhD from RMIT University, Melbourne, Australia in 2018. His main research interests are cybersecurity and privacy preserving analytics.

Center for Computation & Technology
2003 Digital Media Center • Telephone: +1 225/578-5890 • Fax: +1 225/578-8957