به نام خدا

سخنرانی آزمایشگاه امنیت داده و شبکه

Data and Network Security Laboratory

Privacy of Machine Learning Models

Dr. Reza Shokri

Dr. Reza Shokri is joining the computer science department at National University of Singapore (NUS), as assistant professor, this summer. His research focuses on quantitative analysis of privacy, as well as design and implementation of privacy technologies for practical applications. Recently, he has focused on privacy-preserving generative models and privacy in machine learning. He received his PhD from EPFL.

In this talk, he will present their approach for investigating how machine learning models leak information about the individual data records on which they were trained. He will demonstrate how to build a successful inference attack on different classification models e.g., trained by commercial "machine learning as a service" providers such as Google and Amazon.

زمان: شنبه ۶ خرداد ساعت ۹:۱۵

مکان: دانشگاه شریف، دانشکده مهندسی کامپیوتر، طبقه چهار، سالن خوارزمی

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.