Computer Science
Seminar

Scalable and Privacy-Preserving Searchable Cloud Data Services

Ming Li
Utah State University

Abstract: Cloud computing is envisioned as the next generation architecture of IT enterprises, which provides convenient remote access to massively scalable data storage and application services. Despite the clouds promise for huge potential economical savings, its benefits may not be fully realized, due to wide public concerns that users private data may be involuntarily exposed to or mishandled by the cloud providers. Although end-to-end encryption has been proposed as a promising solution for secure cloud data storage, how to effectively support flexible data utilization such as searches over encrypted cloud data becomes a primary challenge, which is the key toward building full-fledged privacy-assured cloud data storage. In this talk, I will first identify the system requirements and challenges in privacy-preserving searchable outsourced cloud data services, that is to simultaneously achieve privacy assurance (data and query confidentiality), practical efficiency (scalable with large volumes of data), and high usability (flexible query functionalities). Among these goals, privacy and the other two are often in conflict with each other and our research aims at finding a better tradeoff. As an example, I will present our recent work on privacy-preserving multi-keyword ranked search supporting similarity-based ranking. The proposed approach integrates novel cryptographic primitives with information-retrieval principles and efficient data structures. A best-effort privacy model is adopted while much faster-than-linear search time is achieved in an empirical sense. Finally, I will outline some future challenges that need to be resolved to make privacy-preserving searchable cloud data service a reality.

Bio:
Ming Li is an Assistant Professor in the Computer Science Department at Utah State University. He received his Ph.D. in Electrical and Computer Engineering from Worcester Polytechnic Institute in 2011. His current main research interest is cyber security and privacy, with emphases on security and privacy in cloud computing and big data, security in wireless networks and cyber-physical systems.

Monday, December 9, 2013, 4:00 pm
Mathematics and Science Center: W301

Mathematics and Computer Science
Emory University