Department of Computer Science

COMPUTER SCIENCE SEMINAR SERIES

Privacy-Assured Large-Scale Navigation from Encrypted Approximate Shortest Path Recommendation

SPEAKER **Mr SHI Zhenkui**

PhD Student
Department of Computer Science
City University of Hong Kong
Hong Kong

DATE 28 December 2017 (Thursday)
TIME 4:00 pm - 4:30 pm
VENUE G7315, 7th Floor, Green Zone
Yeung Kin Man Academic Building
City University of Hong Kong
83 Tat Chee Avenue
Kowloon Tong

ABSTRACT

As the fast-paced market of smart phones, navigation application is becoming more popular especially when traveling to a new place. As a key function, shortest path recommendation enables a user routing efficiently in an unfamiliar place. However, the source and destination are always critical private information. They can be used to infer a user's personal life. Sharing such information with an app may raise severe privacy concerns.

In this paper, we propose a practical navigation system that preserves user's privacy while achieving practical shortest path recommendation. The proposed system is based on graph encryption schemes that enable privacy assured approximate shortest path queries on large-scale encrypted graphs. We first leverage a data structure called a distance oracle to create sketch information, and we further add path information to the data structure and design three structured encryption schemes. The first scheme is based on oblivious storage. The second scheme takes advantage of the latest cryptographic techniques to find the minimal distance and achieves optimal communication complexity. The third scheme adopts homomorphic encryption scheme and achieves efficient communication overhead and computation overhead on the client side. We also evaluated our construction. The results show that the computation overhead and communication overhead are reasonable and practical.

This paper was presented at the 13th International Conference on Mobile Ad-hoc and Sensor Networks (IEEE MSN) 2017, December 17-19, Beijing, China.

Supervisor: Dr WANG Cong

Research Interests: Cloud Computing Security, Secure Computation, Mobile Security and Privacy

All are welcome!

In case of questions, please contact Dr WANG, Cong at Tel: 3442 2010, E-mail: congwang@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/news/seminars/seminars.html.