Jingzhou Luo
MS
CprE
Major Professor: Yong Guan

A Location Privacy Protocol for Mobile Applications

To address the location privacy concerns related to the Location Based Service (LBS), we design an encryption protocol called Location Query over Encrypted Data (LQED). Based on the searchable encryption techniques, we propose two versions of LQED: subset based LQED and range based LQED. Both versions allow mobile applications to encrypt their geological location x into a ciphertext c before submitting it to an untrusted location information broker. Suppose a location information provider has an item, for instance a coupon, is associated with a set of locations L. The provider would generate an asymmetric key pair and create a trapdoor T for that L. That trapdoor T is sent to the untrusted broker mentioned before. The broker may use that trapdoor T to decrypt the ciphertext c whose attribute is the user location x. If the user location x is near any location in L, the decryption will be successful.

We formally define the problem and give detailed construction of those two versions LQED. We implement those two versions and build a proof-of-concept Android application. The practical performance of our construction is also studied. To our best knowledge, our proposal is the first initiation of preserving location privacy using searchable encryption technique. Non-third-party based LBS has very few mature solutions. Private Information Retrieval is one of them, but it suffers some practical performance issues. Our solution would be a secure alternative for it.