# Privacy-Preserving Aggregate Queries for Optimal Location Selection

## ABSTRACT

Today, vast amounts of location data are collected by various service providers. The location data owners have a good idea of where their customers are most of the time. Other businesses also want to use this information for location analytics, such as finding the optimal location for a new branch. However, location data owners cannot directly share their data with other businesses, mainly due to privacy and legal concerns.

## EXISTING SYSTEM

Understanding the whereabouts of current and potential customers can provide valuable insights for location-based services, facility location, and competitive business decisions. Increasing amounts of location data from mobile services, applications, and network operators have introduced exciting opportunities for location enhanced business analytics. The approaches presented in the marketing and operations research literature commonly assume that a business that wants to do analysis owns the data about it. However, this is rarely the case. Location data is typically collected by mobile telecommunication operators and service providers, such as Foursquare. These data owners seek ways to enable other businesses to run location based analytics queries without violating their customers' privacy. Thus, one needs to prevent the location-based service providers from tracking their customers individually, while still allowing other businesses to obtain useful information. Similarly, businesses do not want to share their customer lists with location-based service providers.

## Disadvantages

- Information leak about any single user.
- Server is unaware of the query result and the queries return aggregate results, some queries may leak information about users.

## PROPOSED SYSTEM

We proposed novel protocols for privacy-preserving analysis of location data in a location-based service provider (referred as the server) by a business (referred as the client) as a service. We defined three queries addressing different objectives in optimal location selection:

- to minimize the average distance between each user and her closest facility,
- to minimize the maximum distance between a user and her closest facility.
- to uniformly distribute the workload in facilities.

We developed two homomorphic encryption-based solutions:

- a server-based solution, in which most of the computation is performed by the server, and hence the workload of the client is low.
- a clientbased solution, in which the client performs the majority of the computation during the setup phase (which only occurs once) and after completion of the setup phase, all queries are processed quickly.

We showed that the proposed protocols keep the client's user list and the query result hidden from the server, and the location information stored at the server hidden from the client. The security provided by all protocols relies on the underlying security of the Paillier cryptosystem (which relies on the decisional composite residuosity assumption).

### Advantages

- Homomorphic encryption and differential privacy together to guarantee privacy of individuals during query processing.
- The proposed protocols are practical, efficient, and scalable.

## SOFTWARE REQUIREMENTS

| | | |
|---|---|---|
| Front-end | : | JSP |
| Back-End | : | MySQL |
| Server | : | Tomcat Server |
| OS | : | WINDOWS 7/above |

## HARDWARE REQUIREMENTS

| | | |
|---|---|---|
| PROCESSOR | : | CORE i3 |
| RAM | : | 512MB-2GB |
| HARD DISK | : | 40GB |