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.

- In this paper, we propose privacy-preserving solutions in which location-based queries can be executed and answered by location data owners without sharing their data with other businesses and without accessing the customer list of the businesses that send the query.
- We utilize a partially homomorphic cryptosystem as the building block of the proposed protocols. We prove the security of the protocols in semi-honest threat model. We also explain how to achieve differential privacy in the proposed protocols and discuss its impact on utility.
- We evaluate the performance of the protocols with real and synthetic datasets and show that the proposed solutions are highly practical.

EXISTING SYTEM

- To be consistent, in this paper we refer the location data owner as the server, and the business that requests queries as the client. We refer their customers as the users of the server and the users of the client.
- The client has existing facilities, such as branches of a bank, and aims to find the optimal location for the new one among several candidates.
- The client is able to request a fundamental class of queries that can be used in optimal location selection.
- In these queries, the client only obtains aggregate information about locations of its users without learning the location of any specific user.

- The client has several candidates for the new facility and it can request the queries for each candidate location and select the best one. A simple example to these aggregate queries is average distance query, in which the client retrieves the average distance of its users to their nearest facilities. The nearest facility of each user is the facility that has the minimum distance to that user.

Disadvantages

- Increasing amounts of location data from mobile services
- To prevent informa-tion leak about any single user, we also satisfy differential privacy in our protocols by adding controlled noise to the query result

PROPOSED SYSTEM

- We introduce a practical setting in which the client (e.g., a business) runs a useful class of location-based queries on the database of the server (e.g., a location-based service provider) without violating the privacy of individuals involved both in the client and the server side.
- 2) We enhance facility location problems by remov-ing the assumption that the customer locations are known to the businesses. With the proposed solu-tions, a business can find the best location for a new facility among several candidates without knowing its customer locations.
- 3) We introduce two novel query processing protocols for three different types of queries such as RNN cardinality query, average distance query, and max-imum distance query that are used as a service to identify optimal facility location.

- 4) The proposed protocols take advantage of using a potential superset of user space to hide the list of users of both parties. Our solution does not use any computationally expensive cryptographic com-parisons such as private equality testing or private set intersection. The performance evaluations show that the proposed protocols are practical, efficient, and scalable. For instance, when the server has 25 million users, executing privacy-preserving RNN cardinality query takes around only 10 seconds on a modest computer.

Advantages

- Minimizing the average distance between each user and her closest facility, and
- Minimizing the maximum distance between a user and her closest facility

SYSTEM REQUIREMENT

- **HARDWARE REQUIREMENT:**
- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Sony.
- Ram : 512 Mb.

CONT..

- **SOFTWARE REQUIREMENT:**
- Operating system : Windows XP/7/8
- Coding Language : ASP. Net with C#/Java

Conclusion

- We proposed novel protocols for privacy-preserving anal-ysis 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:
- (i) to minimize the average distance between each user and her closest facility,
- (ii) to minimize the maximum distance between a user and her closest facility, and
- (iii) to uniformly distribute the workload in facilities

Reference

- [1] J. Benaloh. Dense probabilistic encryption. In Proceedings of the Workshop on Selected Areas of Cryptography, pages 120–128, 1994.
- [2] J. Cardinal and S. Langerman. Min-max-min geometric facility location problems. In Proc. European Workshop on Computational Geometry (EWCG'06), pages 149–152, 2006.
- [3] Z. Chen, Y. Liu, R. C.-W. Wong, J. Xiong, G. Mai, and C. Long. Efficient algorithms for optimal location queries in road networks. In Proceedings of the 2014 ACM SIGMOD international conference on Management of data, pages 123–134. ACM, 2014.