A Novel Scheme For Privacy-Preserving and Content-Protecting Location Based Queries

1M. Sreenivasulu, 2Rajendra Chadalawada
1, 2Department of CSE, Audisankara College of Engineering and Technology, Gudur, AP, INDIA

Abstract: In this paper we present a solution to one of the location-based query problems. This problem is defined as follows: (i) a user wants to query a database of location data, known as Points Of Interest (POIs), and does not want to reveal his/her location to the server due to privacy concerns; (ii) the owner of the location data, that is, the location server, does not want to simply distribute its data to all users. The location server desires to have some control over its data, since the data is its asset. We propose a major enhancement upon previous solutions by introducing a two stage approach, where the first step is based on Oblivious Transfer and the second step is based on Private Information Retrieval, to achieve a secure solution for both parties. The solution we present is efficient and practical in many scenarios. We implement our solution on a desktop machine and a mobile device to assess the efficiency of our protocol. We also introduce a security model and analyse the security in the context of our protocol. Finally, we highlight a security weakness of our previous work and present a solution to overcome it.

I. INTRODUCTION:

There are increasing mobile phone users worldwide. So location technologies can be currently used by wireless carrier operators to provide a good forecast of the user location. Now a days, number of users are use location based services which can provide location-aware information Location Based Services (LBSs), also known as location dependent information services (LDISs), have been recognized as an important context-aware application in pervasive computing environments. Spatial queries are one of the most important LBSs. According to spatial constraints, spatial queries can be divided into several categories including nearest neighbor (NN) queries and window queries. An NN query is to find the nearest data object with respect to the location at which the query is issued (referred to as the query location of the NN query). For example, a user may launch an NN query like "show the nearest coffee shop with respect to my current location." On the other hand, a window query is to find all the objects within a specific window frame. An example window query is "show all restaurants in my car navigation window." In general, a mobile client continuously launches spatial queries until the client obtains a satisfactory answer. For example, a query “show me the rate of the nearest hotel with respect to my current location” is continuously submitted in a moving car so as to find a desired hotel. The naive method answering continuous spatial queries is to submit a new query whenever the query location changes. The naive method is able to provide correct results, but it poses the following problems: High power consumption. The power consumption of a mobile device is high since the mobile device keeps submitting queries to the LBS server. Heavy server load. A continuous query usually consists of a number of queries to the LBS server, thereby increasing the load on the LBS server. Fortunately, in the real world, the queries of a continuous query usually exhibit spatial locality. Thus, caching the query result and the corresponding valid region (VR) in the client side cache was proposed to mitigate the above problems. The valid region, also known as the valid scope, of a query is the region where the answer of the query remains valid. Subsequent queries can be avoided as long as the client is in the valid region.

II. LITERATURE SURVEY:

1 “Protecting privacy against location-based personal identification.”

AUTHORS: C. Bettini, X. Wang, and S. Jajodia

This paper presents a preliminary investigation on the privacy issues involved in the use of location-based services. It is argued that even if the user identity is not explicitly released to the service provider, the geo-localized history of user-requests can act as a quasi-identifier and may be used to access sensitive information about specific individuals. The paper formally defines a framework to evaluate the risk in revealing a user identity via location information and
presents preliminary ideas about algorithms to prevent this to happen.

2. “Measuring query privacy in location-based services,”

AUTHORS: X. Chen and J. Pang.

The popularity of location-based services leads to serious concerns on user privacy. A common mechanism to protect users' location and query privacy is spatial generalization. As more user information becomes available with the fast growth of Internet applications, e.g., social networks, attackers have the ability to construct users' personal profiles. This gives rise to new challenges and reconsideration of the existing privacy metrics, such as k-anonymity. In this paper, we propose new metrics to measure users' query privacy taking into account user profiles. Furthermore, we design spatial generalization algorithms to compute regions satisfying users' privacy requirements expressed in these metrics. By experimental results, our metrics and algorithms are shown to be effective and efficient for practical usage.

3. “Private information retrieval,”

AUTHORS: B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan

Publicly accessible databases are an indispensable resource for retrieving up-to-date information. But they also pose a significant risk to the privacy of the user, since a curious database operator can follow the user’s queries and infer what the user is after. Indeed, in cases where the users’ intentions are to be kept secret, users are often cautious about accessing the database. It can be shown that when accessing a single database, to completely guarantee the privacy of the user, the whole database should be down-loaded; namely n bits should be communicated (where n is the number of bits in the database). In this work, we investigate whether by replicating the database; more efficient solutions to the private retrieval problem can be obtained. We describe schemes that enable a user to access replicated copies of a database (k $ 2) and privately retrieve information stored in the database. This means that each individual server (holding a replicated copy of the database) gets no information on the identity of the item retrieved by the user. Our schemes use the replication to gain substantial saving. In particular, we present a two-server scheme with communication complexity O(n1/3).

4. “A public key cryptosystem and a signature scheme based on discrete logarithms,”

AUTHORS: T. ElGamal

A new signature scheme is proposed, together with an implementation of the Diffie-Hellman key distribution scheme that achieves a public key cryptosystem. The security of both systems relies on the difficulty of computing discrete logarithms over finite fields.

III. MODULES:

1. Users
2. Mobile Service Provider
3. Location Server

3.1. Users:

The users in our model use some location-based service provided by the location server LS. For example, what is the nearest ATM or restaurant? The purpose of the mobile service provider SP is to establish and maintain the communication between the location server and the user. The location server LS owns a set of POI records ri for 1 ≤ i ≤ ρ. Each record describes a POI, giving GPS coordinates to its location (xgps, ygps), and a description or name about what is at the location.

3.2. Mobile Service Provider:

We reasonably assume that the mobile service provider SP is a passive entity and is not allowed to collude with the LS. We make this assumption because the SP can determine the whereabouts of a mobile device, which, if allowed to collude with the LS, completely subverts any method for privacy. There is simply no technological method for preventing this attack. As a consequence of this assumption, the user is able to either use GPS (Global Positioning System) or the mobile service provider to acquire his/her coordinates.

3.3. Location Server:

We are assuming that the mobile service provider SP is trusted to maintain the connection, we consider only two possible adversaries. Each and every one for individual communication direction. We consider the case in which the user is the adversary and tries to obtain more than he/she is allowed. Next we consider the case in which the location server LS is the adversary, and tries to uniquely associate a user with a grid coordinate.

IV. ALGORITHMS:

In this paper we used the following algorithms used: they are for initialization Transfer and PIR protocol. These algorithms explained step by step in the following table.
V. CONCLUSION:

In this paper we have presented a location based query solution that employs two protocols that enables a user to privately determine and acquire location data. The first step is for a user to privately determine his/her location using oblivious transfer on a public grid. The second step involves a private information retrieval interaction that retrieves the record with high communication efficiency. We analysed the performance of our protocol and found it to be both computationally and communicationally more efficient than the solution by Ghinita et al., which is the most recent solution. We implemented a software prototype using a desktop machine and a mobile device. The software prototype demonstrates that our protocol is within practical limits.

Future Scope: Future work will involve testing the protocol on many different mobile devices. The mobile result we provide may be different than other mobile devices and software environments. Also, we need to reduce the overhead of the primalty test used in the private information retrieval based protocol. Additionally, the problem concerning the LS supplying misleading data to the client is also interesting. Privacy preserving reputation techniques seem a suitable approach to address such problem. A possible solution could integrate methods from [15]. Once suitable strong solutions exist for the general case, they can be easily integrated into our approach.


