Privacy- Preserving Location-Based Search Queries Along with Service Similarity

V.Preetham
PG Scholar, Software Engineering,
Department of Information Technology,
Gokaraju Rangaraju Institute of Engineering and
Technology, Telangana, India.

K.Lakshmi Sushma
Assistant Professor,
Department of Information Technology,
Gokaraju Rangaraju Institute of Engineering and
Technology, Telangana, India.

ABSTRACT:

Location-based applications utilize the positioning capabilities of a mobile device to determine the current location of a user, and customize query results to include neighboring points of interests. However, location knowledge is often perceived as personal information. One of the immediate issues hindering the wide acceptance of location-based applications is the lack of appropriate methodologies that offer fine grain privacy controls to a user without vastly affecting the usability of the service. While a number of privacy-preserving models and algorithms have taken shape in the past few years, there is an almost universal need to specify one's privacy requirement without understanding its implications on the service quality. In this paper, we propose a user-centric locationbased service architecture where a user can observe the impact of location inaccuracy on the service accuracy before deciding the geo-coordinates to use in a query. We construct a local search application based on this architecture and demonstrate how meaningful information can be exchanged between the user and the service provider to allow the inference of contours depicting the change in query results across a geographic area. Results indicate the possibility of large default privacy regions (areas of no change in result set) in such applications.

Index Terms:
Privacy-supportive LBS, location privacy, service quality.

1. Introduction:

Location Based Service (LBS) has become one of the most popular mobile applications due to the wide use of Smartphones [1].

An increasing number of communication devices (e.g., mobile phones, PDAs), feature positioning capabilities (e.g. GPS), Users may ask location-dependent queries, such as "find the nearest Hospital", answer of this question is given by Location Based Services (LBS) like Google Maps or Map quest [2]. However, queries may disclose subtle information regarding individuals, including their health condition, their lifestyle habits, political and religious bonding, or may result in gratuitous advertisement (i.e., spam)[2]. Privacy concerns are expected to rise as LBSs become more common. Observe that privacy is not protected by replacing the real user identity with a fake one (i.e., pseudonym), because, in order to process location-dependent queries, the LBS needs the exact location of the querying user[2]. An attacker, which may be the LBS itself, can infer the identity of the query source by associating the location with a particular individual.

This can happen in practice, with the use of a public telephone directory, which includes subscribers' addresses Location based advertising and local search are generating most significant revenues like navigation application and also going forward. The smartphones, equipped with GPS modules, have powerful computation ability to process holders' location information, and this brought the flood of LBS applications in the smartphone ecosystem. A good example is the smartphone camera: if one takes a photo with a smartphone camera, the location where the photo is taken is embedded in the picture automatically, which helps one's recognition [1]. Privacy and usability are two equally important requirements for successful realization of a location-based application. Meanwhile, due to the recent advances in wireless technology, mobile devices (e.g., cell phones, PDAs, laptops) with wireless communication capabilities are increasingly becoming popular [3].

Hence, we are presenting the proof of the emergence of many location-based services.(LBS) that allow users to issue spatial queries from their mobile devices everywhere. Obviously, these applications require a quality spatial data, and this results in an step by step increase in the customers of spatial data acquirers [3]. In this paper we are going to propose an innovative approach that simultaneously ensures both the privacy and the integrity. This is achieved by using space encryption as the basis of our approach and then devising techniques that enable the data users to audit the integrity of the query result for the most important spatial query types: range queries and k -nearest-neighbor queries (k-NN). Our proposed contribution is the MR-tree, an index based on the R*-tree, capable of authenticating arbitrary spatial queries. We show, analytically and experimentally, that the MR-tree is considerably faster to build and consumes less space. The MR-tree combines concepts from MB and R*-trees.

2. Related Work:

Users of location-based services (LBSs) may have serious privacy concerns when using these technologies since their location can be utilized by adversaries to infer privacy-sensitive information about them. In this work, we analyze the mainstream anonymity solutions proposed for LBSs based on k-anonymity, and point out that these do not follow the safe assumptions as per the original definition of k-anonymity. In [5] paper, surveyed that Obfuscation concerns the practice of deliberately degrading the quality of information in some way, so as to protect the privacy of the individual to whom that information refers. discussed the increasing trend of embedding positioning capabilities (e.g., GPS) in mobile devices facilitates the widespread use of Location Based Services.

For such applications to succeed, privacy and confidentiality are essential. Existing privacy enhancing techniques rely on encryption to safeguard communication channels, and onpseudonyms to protect user identities. Nevertheless, the query contents may disclose the physical location of the user. In [8] it is observed that recently, highly accurate positioning devices enable us to provide various types of location-based services. On the other hand, because such position data include deeply personal information, the protection of location privacy is one of the most significant problems in location-based services. In this paper, we propose an anonymous communication technique to protect the location privacy of peer users of location-based services.

3. EXISTING SYSTEM:

There are many kinds of location-sensitive applications. One category is location-based access control. Another class of location-sensitive applications requires users to provide past location proofs such as auto insurance quote in which auto insurance companies offer discounts to drivers who can prove that they take safe routes during their daily commutes, police investigations in which detectives are interested in finding out if a person was at a murder scene at some time, and location-based social networking in which a user can ask for a location proof from the service requester and accepts the request only if the sender is able to present a valid location proof. The common theme across these location sensitive applications is that they offer a reward or benefit to users located in a certain geographical location at a certain time. Thus, users have the incentive to cheat on their locations.

DISADVANTAGES OF EXISTING SYSTEM:

•In the location-sensitive applications there is a lack of secure mechanism to provide their current or past locations to applications and services.

•Although cellular service providers have tracking services that can help verify the locations of mobile users in real time, the accuracy is not good enough and the location history cannot be verified.

4. A Framework for Capturing Location Privacy and Service Quality :

Framework contains the description of a system model that connects privacy, service quality and cloaked information. This model is the basis for subsequent discussions. Figure 1 illustrates this system model[4]. In this main idea is to allow the user to specify it's location, service request and privacy requirements to the cloaking agent. Which then builds the cloaked location (i.e., a larger region that contains the user's true location) and an "imprecise" service request . On collection of this information, the service provider processes the request and sends back the service and feedback to the user. The cloaking agent can either be implemented in the user's device, or provided by a third-party system. In Figure 1 it can be seen that a user can first specify its privacy preferences through a privacy language.

Privacy language, that we are planning to develop, allows a subject to specify her privacy preferences with respect to:

• Locations - a user may specify that when being near to a given object, cloaking is required, and the accuracy requirements. Locations can be logical or physical;

• Other users and service providers - a user may also specify that her presence be made known (or hidden) to specific users and service providers. Inside the cloaking agent, the user's privacy preferences are then forwarded to the policy translator. The policy translator produces a cloaked location based on the precise location of the user and its privacy requirements. For instance, if the user's requirement is "generate a cloaked location that covers five buildings when I am in Area A", the policy translator produces the corresponding cloaked location when it detects the user is in Area A. The policy translator also forwards to the service provider the user's privacy preference concerning other users and service providers if needs. Based on the cloaked location and the service request, the service translator produces an "imprecise" service request that processes cloaked data. Based on the recommendation from the cloaking agent, the user can then decide if the degree of privacy should be reduced. Let us now focus on data modeling, query evaluation, quality and privacy protection issues for this system. A novel architecture for LBS applications that is directed toward revealing privacy/utility tradeoffs to a user before an actual geotagged query is made. Unlike a typical competitive.architecture where the LBS provider does not actively participate in making privacy decisions, a privacy-supportive LBS as a provider willing to provide supplemental information for making "informed" privacy decisions

5. Privacy-Supportive LBS :

There is an increasing doubt about how a LBS provider handles location data. The Location accuracy is indeed a characteristic requirement of the application as a evidence to build an strong market adoption. As only the service provider can maintains the database of queried objects in real time, it is reasonable that differences or similarities in the output of a query can be efficiently computed at the server side. A user is unable to make privacy decisions without this computation. From these comments, a privacy supportive LBS seems both appropriate as well as important. Also it founds that a simple opt-in LBS is not privacy-supportive, as the implications of not using ones geo-location is unavailable to the user.

6. PROPOSED SYSTEM:

We propose a user-centric location based service architecture where a user can observe the impact of location inaccuracy on the service accuracy before deciding the geo-coordinates to use in a query. We construct a local search application based on this architecture and demonstrate how meaningful information can be exchanged between the user and the service provider to allow the inference of contours depicting the change in query results across a geographic area. Results indicate the possibility of large default privacy regions (areas of no change in result set) in such applications.Privacy and usability are two equally important requirements for successful recognition of a location-based application. Privacy (location) is widely defined as a "personally" estimated restriction on when and where someone's position is considered appropriate for disclosure. Existing system searches user query locally using data structure, so query takes time to search result. Also in existing system there is lack of efficiency and also space and time consuming system. For fast and efficient searching technique also space efficient we can propose MR-tree. The MR-tree is considerably faster to build and consumes less space. At the same time, it is much more efficient for query processing and verification. Merkle-tree, which is an authenticated data structure (ADS) that is built on the dataset. Proposed system provides a novel index suitable for location based query search.

ADVANTAGES OF PROPOSED SYSTEM:

We can effectively provide location proofs, significantly preserve the source location privacy, and effectively detect colluding attacks. Mobile local search is demonstrating an upward market trend.

A. Communication Order For a Location Based Query :

The communication setting includes one or more users equipped with GPS-enabled devices, and an LBS provider possessing a database of points-of-interest (POI). These POI may be static or dynamic, as in case of local business listings and as in case of a friend-finder service respectively where users usually check-in/out of the underlying on social-networking platform. Like this in almost all operating LBS applications, user access to the service is supplemented by a geographic tag identifying the position of the user.

Authentication may or may not be necessary to use the service, since many applications are able to provide a better result set in the latter case. The service itself may have requirement of other parameters to be specified, such as searches keywords or profile descriptions. The geographic tag in the query is typically the GPS-coordinates of the user device, but can also be a carefully designed location.

Architecture:

The location disclosure mechanism in a privacysupportiveLBS architecture employs an intermediatecommunication with the LBS. A high-level schematic ofthe communication pattern is depicted in Fig. 1. The userdevice forwards the query to the LBS, albeit uses a highlevelgeneralization of the user's geographic locationin it. This generalization may be derived as per userspecification (say at the level of the city), or obtainedautomatically from the location approximation that aprovider can infer using a cell-towers and wifi-accesspoints database1. In response to this first query phase,the user obtains a service-similarity profile. This profile is a representation of the similarities in the query outputat different geographic locations. The exact form takenby this profile, as well as the data structures employedin computing this profile, may vary from application toapplication.

A location perturbation engine on the userside then determines a noisy location to use based on theser's privacy profile and the retrieved service-similarityprofile. The LBS processes the query with respect to thenoisy location.A user can manually interact with the servicesimilarityprofile to assess which locations have the highest(or acceptable) level of result set similarity, withinthe constraints of the location noise she wants to infuseinto the query. In this case, a good visualization of similarity profile is required. Although this is themost flexible method of putting the trade-off informationto use, such high degree of interaction will affect theusability of the application, specially when queries aremade frequently. Hence, we assume that action axiomshave been provided by the user to make the processautomatic. The privacy profile then states how a locationis to be selected for different categories of applications,their importance, and the relative location sensitivity. Policy specifications such as these, and their integrationinto the decision making process, warrant an extensiveexploration. We will avoid this frontier in this work.

Anaive approach is to allow the user to select a location-sensitivity level (much like choosing the ringer-state ina mobile phone), assess query result accuracy at thecorresponding location granularity (using the similarityprofile), and notify the user if the accuracy drops belowa threshold. Note that the policy executes within auser's device and reveals little or no information on howlocations get chosen.
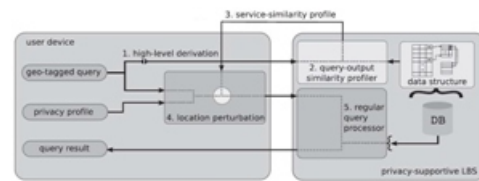

Figure 1. Communication order for a location-based query in the presence of a privacy-supportive LBS.

Conclusion:

Based on the observations from the empirical study,we make the following conclusions on the efficacy ofa privacy-supportive local search application.Precise geo-locations are necessary for result set accuracywhen the queried objects exist as a dense clusterin the search area. It seems unlikely that both locationprivacy and result exactness can be maintained inthis case. A privacy-supportive application would allowthe user to aggressively trade-off the service similarityrequirement to determine a sufficiently large area forlocation perturbation. Given the high density of objects resulting objects can still be expected to be in the nearvicinity.When object density is not dense, location accuracyhas a minor role to play in retrieving relevant results. Aprivacy-supportive application would help identify thelarge default-privacy regions resulting in such situations.Next generation telecommunication systems couldvery well make it possible to quickly (and costeffectively)transfer all information required to infer theservice-contour exactly. Until then, approximate inferencingalgorithms can be used to reduce the communicationoverhead.

References:

[1] J. Sythoff and J. Morrison, Location-Based Services: Market Forecast,2011-2015. Pyramid Research, 2011.

[2] P. Golle and K. Partridge, "On the Anonymity of Home/WorkLocation Pairs," in Proceedings of the 7th International Conference onPervasive Computing, 2009, pp. 390–397.
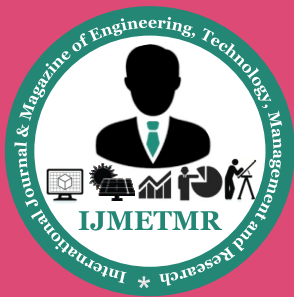
[3] H. Zang and J. Bolot, "Anonymization of Location Data DoesNot Work: A Large-Scale Measurement Study," in Proceedings ofthe 17th Annual International Conference on Mobile Computing andNetworking, 2011, pp. 145–156.

[4] M. Duckham and L. Kulik, "A Formal Model of Obfuscationand Negotiation for Location Privacy," in Proceedings of the 3rdInternational Conference on Pervasive Computing, 2005, pp. 152–170.

[5] H. Kido, Y. Yanagisawa, and T. Satoh, "An Anonymous CommunicationTechnique Using Dummies for Location-Based Services,"in Proceedings of the IEEE International Conference on PervasiveServices, 2005, pp. 88–97.

[6] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, "PreservingUser Location Privacy in Mobile Data Management Infrastructures,"in Proceedings of the 6th Workshop on Privacy EnhancingTechnologies, 2006, pp. 393–412.

[7] M. L. Yiu, C. S. Jensen, X. Huang, and H. Lu, "SpaceTwist: Managingthe Trade-Offs Among Location Privacy, Query Performance,and Query Accuracy in Mobile Services," in Proceedings of the 24thInternational Conference on Data Engineering, 2008, pp. 366–375.

[8] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," inProceedings of the 1st International Conference on Mobile Systems,Applications, and Services, 2003, pp. 31–42.

[9] B. Gedik and L. Liu, "Protecting Location Privacy with Personalizedk-Anonymity: Architecture and Algorithms," IEEE Transactionson Mobile Computing, vol. 7, no. 1, pp. 1–18, 2008.

[10] P. Samarati, "Protecting Respondents' Identities in MicrodataRelease," IEEE Transactions on Knowledge and Data Engineering,vol. 13, no. 6, pp. 1010–1027, 2001.