Service Correspondent for Privacy in Location Based Data Retrieval

Prerana S.Deokar[1], Praveen Barapatre[2]

[1]Department of Computer Engineering, SKN Sinhgad Institute of Technology and Science, Lonavala

[2]Professor, Department of Information Technology, SKN Sinhgad Institute of Technology and Science, Lonavala

Abstract: ***Location Based Application (LBA) provide location based services (LBS) by using queries called location based queries (LBQ). The result of these queries is based on location of mobile user. Privacy and Usability are two important issues of realization of location of user queries. Existing established system(s) developing a User Centric location based service architecture (local search application) where a user can observe the impact of inaccuracy on service accuracy before sending request of geo-coordinates to use in request. This article focuses on Location based services and how location based queries are solved using different methods. This system proposes local search application through which user can put a query and give result according to that query. User can put a query through image instead of text.***

Keywords: Location Based Application(LBA),Location Based Services(LBS),Location Based Queries(LBQ).

1. Introduction

In todays World, Smartphone becomes widely used device. Location of user or object is its geographical position on the earth and such location data is traceable and real time. This information can be catagorized as per longitude, latitude and street address. For location based queries we need to know the geographic domain. Geographic domain is defined by area covered by Mobile Computing Platform. While navigation applications are currently generating the most significant revenues, location-based advertising and local search will be driving the revenues going forward. The legal landscape, unfortunately, is unclear about what happens to a subscribers location data. The nonexistence of regulatory controls has led to a growing concern about potential privacy violations arising out of the usage of a location based application. While new regulations to plug the loopholes are being sought, the privacy conscious user currently feels reluctant to adopt one of the most functional business models of the decade.

Paper discusses how location based queries can be solve in efficient manner and provide accuracy to result. In Location Based System privacy is important issue. Privacy (location) is loosely defined as a personally assessed restriction on when and where someone's position is deemed appropriate for disclosure. To begin with, this is a very dynamic concept. Usability has a two fold meaning1) privacy controls should be intuitive yet flexible and 2 the intended purpose of an application is reasonably maintained. Toward this end, prior research has led to the development of a number of privacy criteria, and algorithm for their optimal achievement. It is worth mentioning that a separate line of research in analyzing anonymous location traces has revealed that user locations are heavily correlated, and knowing a few frequently visited locations can easily identify the user behind a certain trace. The privacy breach in these cases occurs because the location to identity mapping results in a violation of user anonymity. The proposal in this work attempts to prevent the reverse mapping from user identity to user location albeit in a user-controllable manner.

2. Literature Survey

In paper [1], they design one local search application through this user can solve location based queries and exchange information between user and service provider. Cloaking algorithm is used for solving location based query. They propose a novel architecture for LBS applications. The application starts with anchor, a location different from that of user and it start working until an accurate query result can be reported. The work focuses to reduce the communication cost of the repeated querying mechanism.

In paper [2], discuss about new attack on the anonymity of location data. Anonymity is helpful but not perfect tool for preserving location privacy. This paper studies the threat of re-identification and model of privacy. In this paper they use a LEHD (Longitudinal Employer Household Dynamics) dataset.

This paper studies a new attack on the anonymity of location data. Golle et.al show that if the approximate locations of an individual's home and workplace can both be deduced from a location trace, then the median size of the individual's anonymity set in the U.S. working population is 1, 21 and 34,980, for locations known at the granularity of a census block, census track and county respectively. The location data of people who live and work in different regions can be re-identified even more easily.

In paper [4], [5] obfuscation has been achieved through the use of dummy queries or cloaking regions. User hides her actual query among set of additional queries with incorrect locations. The user's actual location is one among the locations in the query set. The paper sets out a formal framework within which obfuscated location-based services are defined. This framework provides a computationally efficient mechanism for balancing an individual's need for high-quality information services against that individual's need for location privacy. Negotiation is used to ensure that a location-based service provider receives only the information it needs to know in order to provide a service of satisfactory quality.

Cheng et al. propose data model to augment uncertainty to location data using circular regions around all objects [6].They does not use precise queries that hide location of user who issue query and probabilistic results. In this paper, we suggest a framework where uncertainty can be controlled to provide high quality and privacy-preserving services, and investigate how such a framework can be realized in the GPS and cellular network systems. Based on this framework, we suggest a data model to augment uncertainty to location data, and propose imprecise queries that hide the location of the query issuer and yields probabilistic results.

Gruteser and Liu proposed the use of spatial and temporal cloaking to obfuscate user locations [7].They creates spatial regions to hide the true location of user.

Ghinita et al. propose a decentralized architecture to construct an anonymous spatial region and eliminate the need for the centralized anonymizer [8].In their approach, mobile nodes utilize a distributed protocol to self-organize into a fault-tolerant overlay network, from which a k-anonymous cloaking set of users can be determined.

3. Existing System

3.1 Contributions

Existing system has two contributions Rinku Dewri et al. first propose a novel architecture which directed towards revealing privacy to a user. Typical architecture in which LBS provider inactive in making privacy decisions. For obtaining user location it is challenging task for that user first consider overview of the impact of using inaccurate locations in some query. After that, the actual query made to service provider is geotagged with a location that the user has chosen to balance result accuracy and privacy.

Second contribution is that design one privacy-supportive LBS application where user can put search term and their location the privacy-supportive LBS provide representation of 10 nearest neighbor result set.

3.2 Architecture

The user put query to the LBS, user uses geographic location in that query. Result to this phase user get service similarity profile.

This profile is collection of homogeneous in the query output at different geographic locations. A location perturbation engine on the user side then determines a noisy location to use based on the user's privacy profile and the retrieved service-similarity profile. The LBS processes the query with respect to the noisy location. A user manually communicate with service similarity profile to assess which locations have higher level of result set similarity.

A naive approach is to allow the user to select a location sensitivity level assess query result accuracy at the corresponding location and notify the user if the accuracy drops below a threshold.

4. Proposed System

Location based system can solve location based queries through local search application. In local search application there are three modules. Modules are User module, Admin module, Local search application.

4.1 Problem Statement

In the traditional usage of a local search application, the user would communicate a search keyword to the provider, and retrieve a ranked list of records matching the search term. In proposed system developed one application through which user can put query and according to user location application will display result. Additional instead of giving query user can put image of location and user will get result. After getting result re-rank the result.

4.2 User Module

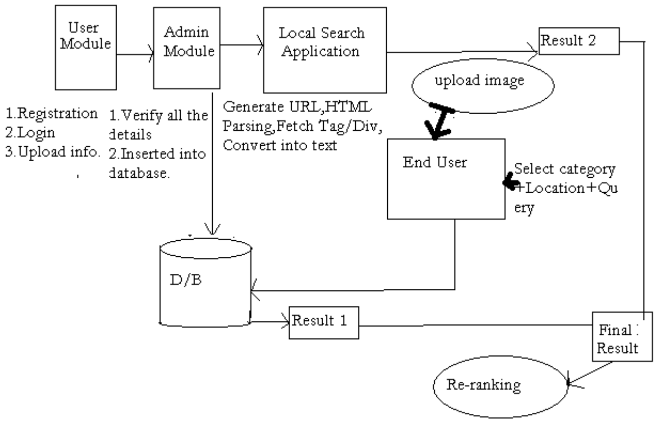
In this module a new user can register by giving his details. After providing the details admin will verify all the details. If user already register itself then he can login directly. All the details are stored on main database.

4.3 Admin Module

In this module admin will verify and validate user details and store data on main database.

4.4 Local Search Application

In this phase user can put their query and this application will solve it. End user select category that which type of information he wants then enters location, query. This information store on main database. After that local search application will generate URL in form of web services and send it to browser then HTML Parsing will perform then it will fetch particular Tag/Div and convert it into text format. Whatever result will come that is result 2.After adding result 1 and result2 user will get final result.



Above fig. shows the architecture of proposed system new user register and upload information and that information will verify by admin.

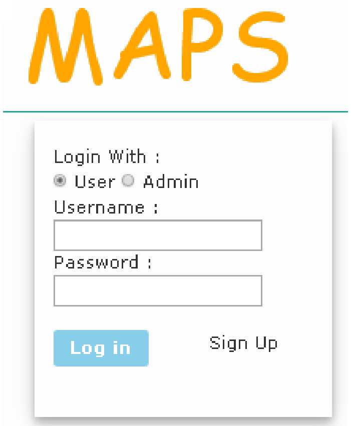
4.5 Mathematical Model

Let S be a technique to Location based Search Query.
Such That S= {I,F,O} Where,
I represents the set of inputs:
I= {D, W}
D= Location Privacy.
W= Service Quality.
F is the set of functions:
F= {T,F,M}
T= Privacy Supportive LBS
F= Service Contour Interfacing
M= Privacy Supported Local Search

O is the set of outputs:
O= {C}
C= Local Search Result

5. Result

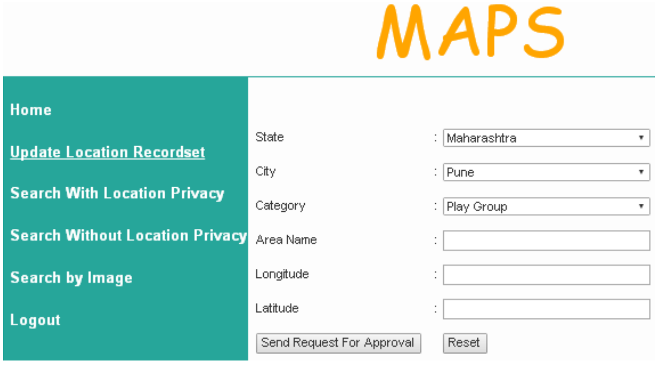
In this application after entering user name and password five options are shown. By clicking update recordset option user can update the location into database .



Login With :
● User ○ Admin
Username :
Password :

Figure 1: Login Page

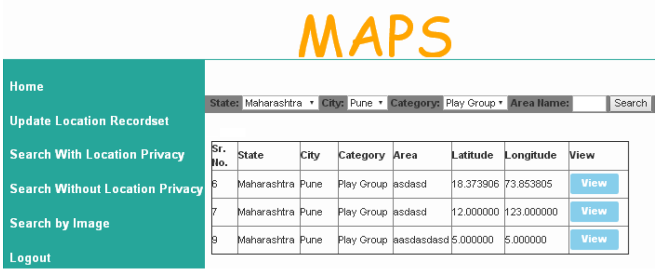
After clicking on update location recordset option user can see following window.


MAPS
Home
Update Location Recordset
Search With Location Privacy
Search Without Location Privacy
Search by Image
Logout
Send Request For Approval
Reset

State	:	Maharashtra
City	:	Pune
Category	:	Play Group
Area Name	:	
Longitude	:	
Latitude	:	

Figure 2: Update Location Recordset

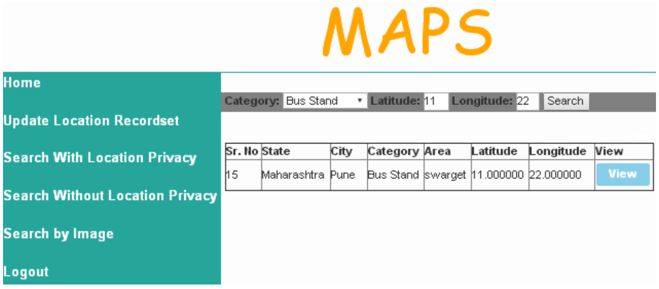
For Searching there are two options search with privacy and search without privacy.


MAPS
Home
Update Location Recordset
Search With Location Privacy
Search Without Location Privacy
Search by Image
Logout
Search

State: Maharashtra City: Pune Category: Play Group Area Name:

Sr. No.	State	City	Category	Area	Latitude	Longitude	View
6	Maharashtra	Pune	Play Group	asdasd	18.373906	73.853805	View
7	Maharashtra	Pune	Play Group	asdasd	12.000000	123.000000	View
9	Maharashtra	Pune	Play Group	aasdasdasd	5.000000	5.000000	View

Figure 3: Search with Privacy

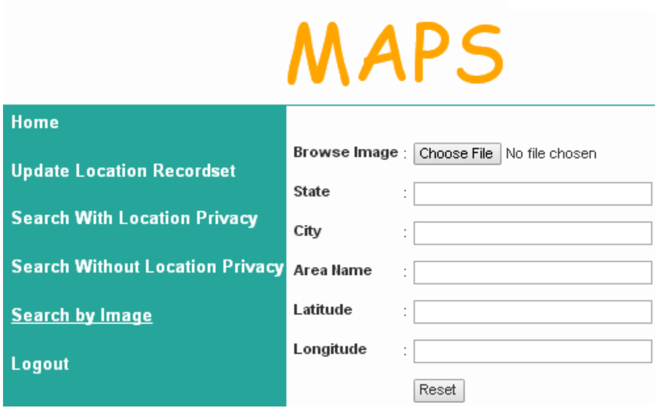

MAPS
Home
Update Location Recordset
Search With Location Privacy
Search Without Location Privacy
Search by Image
Logout
Search

Category: Bus Stand Latitude: 11 Longitude: 22

Sr. No	State	City	Category	Area	Latitude	Longitude	View
15	Maharashtra	Pune	Bus Stand	swarget	11.000000	22.000000	View

Figure 4: Search without privacy

By providing query through image for that following screen will apper


MAPS
Home
Update Location Recordset
Search With Location Privacy
Search Without Location Privacy
Search by Image
Logout
Choose File
Reset

Browse Image	:	No file chosen
State	:	
City	:	
Area Name	:	
Latitude	:	
Longitude	:	

Figure 5: Image capturing screen

6. Conclusion

Rinku Dewri and Ramakrishna Thurimella proposes novel architecture for LBS (Location Based Services) applications. This architecture provide the result of user query but this application does not provide privacy and accuracy to user query. Precise geolocations are necessary for result set accuracy when the queried objects exist as a dense cluster in the search area.

This system explains how we can improve privacy and accuracy of user query. This system can provide user query through image of locations. Additional we can re-rank the result of query.

To determine large area for location perturbation location privacy and result exactness can be maintained and user can tradeoff the service similarity requirement.

References

[1] Rinku Dewri and Ramakrisha Thurimella, Exploiting Service Similarity for Privacy in Location-Based Search Queries. Proc. IEEE Transaction on Parallel and Distributed Systems,Vol.25,pp 374-383,2014.

[2] P. Golle and K. Partridge, On the Anonymity of Home/Work Location Pairs, Proc. Seventh Intl Conf. Pervasive Computing,pp. 390-397, 2009.

[3] H. Zang and J. Bolot, Anonymization of Location Data Does Not Work :A Large-Scale Measurement Study, Proc. 17th Ann. Intl Conf. Mobile Computing and Networking, pp. 145-156, 2011.

[4] M. Duckham and L. Kulik, A Formal Model of Obfuscation and Negotiation for Location Privacy, Proc. Third Intl Conf. Pervasive Computing,pp. H. Kido, Y. Yanagisawa, and T. Satoh, “An Anonymous Communication Technique Using Dummies for Location-Based Services,” Proc. IEEE Int’l Conf. Pervasive Services, pp. 88-97, 2005.

[5] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, Preserving User Location Privacy in Mobile Data Management Infrastructures,Proc. Sixth Workshop PrivacyEnhancing Technologies,pp. 393-412, 2006.

[6] M. Gruteser and D. Grunwald, Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking,Proc.First Intl Mobile Systems, Applications and Services, pp. 31-42, 2003.

[7] G. Ghinita, P. Kalnis, and S. Skiadopoulos, PRIVE: Anonymous Location-Based Queries in Distributed Mobile Systems, Proc. 16th Intl Conf. World Wide Web,pp. 371-380, 2007.Conf.Mobile Systems,Applications, and Services, pp. 31-42,2003.

[8] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, Preventing Location-Based Identity Inference in Anonymous Spatial Queries, IEEE Trans. Knowledge and Data Eng., vol.19, no. 12, pp. 1719-1733, Dec.2007

[9] G. Ghinita, K. Zhao, D. Papadias, and P. Kalnis, A Reciprocal Framework for Spatial k-Anonymity, J. Information Systems vol. 35, no. 3. pp. 299-314, 2010

[10] A. Beygelzimer, S. Kakade, and J. Langford, Cover Trees for Nearest Neighbor, Proc. 23rd Intl Conf. Machine Learning, pp. 97-104, 2006.

[11] P. Samarati, Protecting Respondents Identities in Microdata Release,IEEE Trans. Knowledge and Data Eng., vol. 13, no. 6, pp. 1010-1027,Nov. 2001.

[12] B. Gedik and L. Liu, Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms, IEEE Trans.Mobile Computing vol. 7, no. 1, pp. 1-18, Jan. 2008.

[13] M.L. Yiu, C.S. Jensen, X. Huang, and H. Lu, SpaceTwist:Managing the Trade-Offs among Location Privacy, Query Performance, and Query Accuracy in Mobile Services, Proc.24th Intl Conf. Data Eng., pp. 366- 375, 2008.