ISSN: 2321-7782 (Online)
Volume 3, Issue 6, June 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Accomplishing Service Similarity in User centric Location Based Queries for Privacy

Pushpalata Bhagadkar[1]
G.H. Raisoni college of Engineering and Management
Ahemadnagar, India,
Savitribai Phule Pune University, Pune - India

Dr. Tanuja Dhope[2]
Comp.Dept.,G.H. Raisoni college of Engineering and Management, Pune, India,
Savitribai Phule Pune University, Pune - India

Abstract: ***Location-Based Service (LBS) becomes increasingly popular with the dramatic growth of smartphones and social network services (SNS), and its context-rich functionalities attract considerable users. Most of LBS providers make use of users' location information to provide them convenience and useful functions. Location based applications exploits the focusing capabilities of mobile device to determine the current position of user, and specifies the query results to capture the neighboring points of interest. In this paper the propose system is an novel approach that simultaneously ensures both the privacy and the integrity. This is achieved by using space encryption as the basis of this approach and then conceives techniques that enable the data users to audit the integrity of the query result for the range queries and k -nearest-neighbor queries (k NN). And it can be accomplish by using the MR-tree, an index based on the R*-tree, capable of authenticating arbitrary spatial queries. Here it can be shown, analytically and experimentally, that the MR-tree is considerably faster to build and consumes less space.***

Keywords: Service quality , location privacy , Privacy-supportive LBS, data privacy, MR*tree.

I. INTRODUCTION

Location Based Service (LBS) has become one of the most popular mobile applications due to the wide use of Smartphones [1]. A location-based service provides valuable applications and services to mobile users. To encounter these services, users must reveal their location to service providers. This raises privacy concern, location records, when analyzed, can reveal sensitive facts about an individual, such as business connections, political affiliations or medical conditions. Misuse of location data can lead to damaged reputation, harassment, mugging, as well as attacks on an individual's home, friends or relatives. Privacy policies and legislation address some of these concerns. But protection mechanisms placed in policy or laws are only effective when data collectors are honest and trusted. They offer no protection against a dishonest collector, or one whose data is compromised by malware, laptop theft or a weak password. To minimize privacy concerns, the best practice is to collect the minimum amount of information needed. For location-based services, this principle of minimal collection.

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].

Privacy and usability are two equally important requirements for successful realization of a location-based application. Meanwhile, 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 these results in an step by step increase in the customers of spatial data acquirers [3].

In this paper the proposed novel approach simultaneously ensures both the privacy and the integrity. This is achieved by using space encryption as the basis of this approach and then composed techniques that enable the data users to ensure the integrity of the query result for the most important spatial query types: range queries and k -nearest-neighbor queries (k NN). The proposed contribution is the MR-tree, an index based on the R*-tree, capable of authenticating arbitrary spatial queries. MR-tree is considerably faster to build and consumes less space. The MR-tree combines concepts from MB and R*-trees.

The organization of this paper is as follows. Section I describe the introduction followed by related Section III briefs out the privacy-supportive LBS. In detail explain about the proposed system is given in Section IV .The simulation result has been discussed in section V which is followed by conclusion in section VI.

II. Related Work

In [4] paper, shown that Obfuscation concerns the degrading the quality of information in some way, to protect the privacy of the individual to whom that information refers. In this paper, it is explained that obfuscation is an important technique for protecting an individual's location privacy within a pervasive computing environment. The paper gives a formal

framework within which obfuscated location-based services are defined and it provides a computationally efficient mechanism for balancing an individual's need for high utility information services against that individual's need for location privacy. Deliberation is used to ensure that a location-based service provider that receives the information only it needs to know in order to provide a service of satisfactory quality. The results of this work have indications for numerous applications of mobile and location-aware systems, as they offers some new theoretical foundation for locating the privacy concerns that are acknowledged to be retarding the widespread acceptance and use of location-based services.

In [5] paper, surveyed that Many applications benefit from user location data, but it also raises privacy concerns. Anonymization able to protect privacy, but identities can sometimes be deduce from anonymous data. This paper researches a new attack on the anonymity of location data. We show that if the approximate locations of an individual's home and workplace can both be inferred from a location trace, then the median size of the individual's anonymity set. The location information of people who live and work in different regions can be re identified more easily. In this results shows that the threat of re identification for location data or information is much greater when the individual's home and work locations can both be deduced from the data. To preserve anonymity, it will offer guidance for obfuscating location traces before they are disclosed.

In [6] paper, 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 privacy and confidentiality are essential to succeed, Existing privacy enhancing techniques depends on encryption to safeguard and protect the communication channels, and on pseudonyms to protect user identities. Nevertheless, the query contents may reveal the physical location of the user.

In [7] paper ,shown that 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. It has failed to maintain the privacy of users. The location data of the people who live and work in different areas can be re identified even more easily. 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 concerns of location privacy are one of the most significant problems in location-based services. In this paper, an anonymous communication technique proposed to protect the location privacy of the users of location-based services.

III. 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.

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.

B. System Architecture

A privacy-supportive LBS architecture employs an intermediate communication with the LBS In the location disclosure mechanism the communication pattern is presented in Fig. 2. The user device forwards the query to the LBS, albeit uses a high-level generalization of the user's geographic location in it. This generalization can be derived as per user-specification, or obtained automatically from the location approximation. A provider can conclude using a cell-towers and Wi-Fi-access point database.

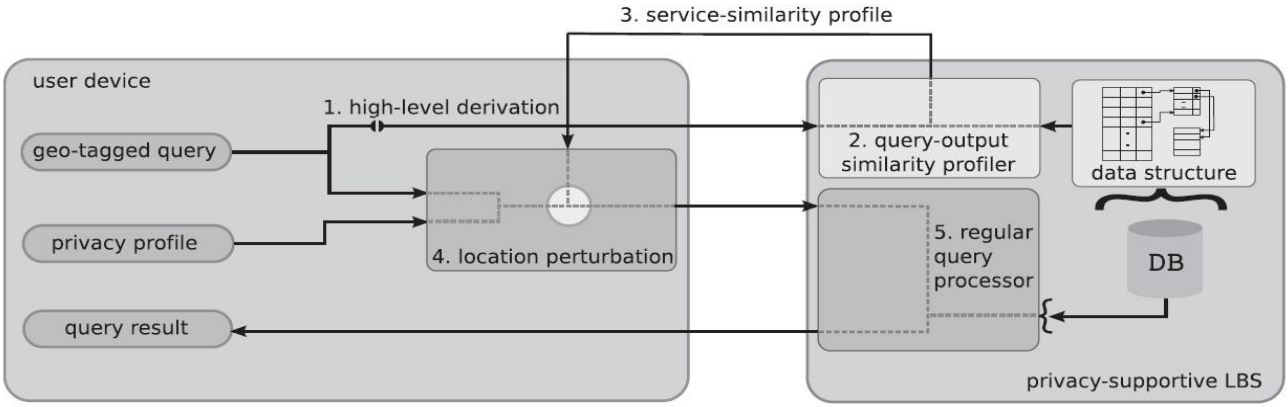


Fig. 1. Communication order for a location-based query in the presence of privacy-supportive LBS

As response to this first query phase, the user obtains a service-similarity profile. This profile is a representation of the similarities in the query output of different geographic locations. The exact form taken by this profile, as well as the data structures employed in computing this profile, may vary from application to application.

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 can manually interact with the service-similarity profile to assess which locations have the highest (or acceptable) level of result set similarity, within the constraints of the location noise. Although this is the most flexible method of putting the tradeoff information to use, such high degree of interaction will affect the usability of the application, especially when queries are made frequently. Hence, we assume that action axioms have been provided by the user to make the process automatic. The privacy profile then states how a location is to be selected for different categories of applications, their importance, and the relative location sensitivity. Policy specifications such as these, and their integration into the decision making process, warrant an extensive exploration. A naive

approach is to allow the user to select a location sensitivity level, assess query result accuracy at the corresponding location granularity the similarity profile.

IV. PROPOSED SYSTEM

Privacy and usability are two equally important requirements for successful recognition of a location-based application. Existing system searches user query locally using data structure, so query takes time to search result. 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.. 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 [10].

An alternative anonymity property, LBS (k,T)-anonymity, that ensures anonymity of a user's query against an attacker who knows about the issuance of the user query within a time window.. The present a framework for preventing location based identity inference of users who issue spatial queries to Location Based Services. Transformation's based on the well-established K -anonymity concept to compute exact answers for range and nearest neighbor search, without revealing the query source. Extensive experimental studies suggest that the proposed techniques are applicable to real-life scenarios with numerous mobile users. As The MR-tree is considerably faster to build and consumes less space.

Algorithm

RangeQuery (Query Q, MR_Node N) // LBS

1. Append [to VO

2. For each entry e in N // entries must be enumerated in original order

3. If N is leaf

4. Append e.data to VO

5. Else // N is internal node

6. If e.MBR overlaps Q, Range Query (Q, e.pointer)

7. Else append e.MBR, e.hash to VO // a pruned child node

8. Append] to VO

A hash value is calculated on the concatenation of the binary representation of all objects in the node.

Internal nodes contain entries of the form (*pi*, *MBRi*, *hi*), signifying the pointer, minimum bounding rectangle and hash value of the *i*th child, respectively.

The hash value of root node(*hroot)* is signed by the data owner and stored with the tree.

1)To process a range query Q

A. The LBS invokes *Range Query* (*root*, *Q*),

B. The algorithm evaluates the verification object. by following a depth-first traversal of the MR-tree.

2)The VO contains three types of data

- all objects in each leaf node visited (Line 4),
- the MBR and hash values of pruned nodes (Line 7),
- special tokens [and] that mark the scope of a node (Lines 1 and 8)
- New entries are always appended at the end of the VO.

1)Example

Consider, for instance, query Q, Similar to conventional R-trees, Range Query starts from the root and visits recursively all entries that overlap the shaded rectangle: N1, N4, N2, N5. After termination, tokens signify the contents of a node; for instance, the component [[(MBR_N3, hash_N3), [P4, P5, P6]]] corresponds to the first root entry (N1), and the rest of the VO to the second one (N2).

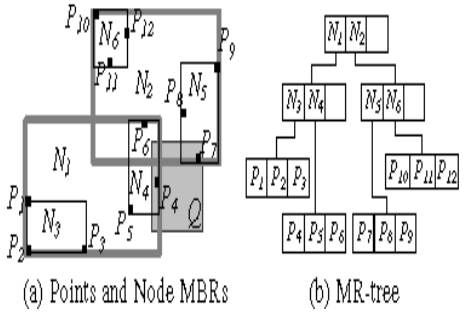


Fig 2. MR* tree

The LBS transmits the *VO* and the root signature *sroot* to the client. Note that the actual result (e.g., *P4*, *P7*) is part of the *VO*.

Mathematical Model

Let S be the system which use for fine grain privacy controls to a user without vastly affecting the usability of the service. In this system the proposed architecture is a user-centric location based service architecture. It constructs a local search application based on MR tree architecture and demonstrate how meaningful information can be exchanged between the user and the service provider.

$$S = \{UQ, SP, MR, LP, QR\}$$

Where S=System,

UQ=The user device forwards the query to the LBS

SP = Service Similarity Profile, This profile is a representation of the similarities in the query output at different geographic locations

MR = Merkel tree, to develops an authenticated data structure (ADS) called Merkle R-tree (MR-tree) based on R*-tree and Merkle tree.

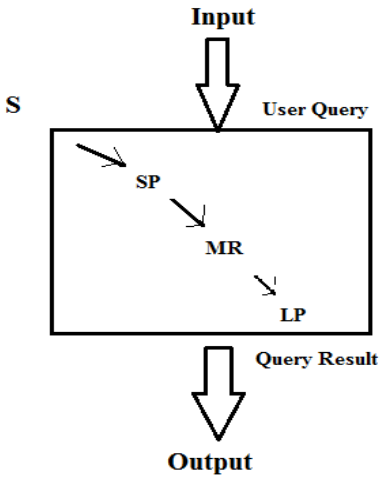


Fig 3. Query Processing

2)UQ (User Query)

The user device forwards the query to the LBS, and by using a high-level generalization of the user's geographic location. This generalization may be derived as per user-specification (say at the level of the area), or obtained automatically from the location approximation that a provider can be deduce using a cell-towers and Wi-Fi access points database.

3)MR (Merkle Tree)

The MR-tree is an combined concept of MB and R*-trees the node structure. Leaf nodes are identical to the R*-tree: each entry Ri corresponds to a data object. A hash value is computed on the concatenation of the binary representation of all objects in the node. Internal nodes contain entries of the form (*pi*, *MBRi*, *hi*), signifying the pointer, minimum bounding rectangle and hash value of the *i*th child, respectively.

(a) Leaf Node (b) Internal Node

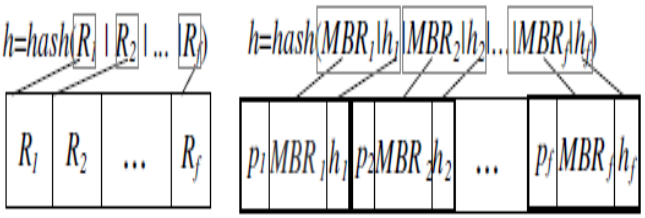
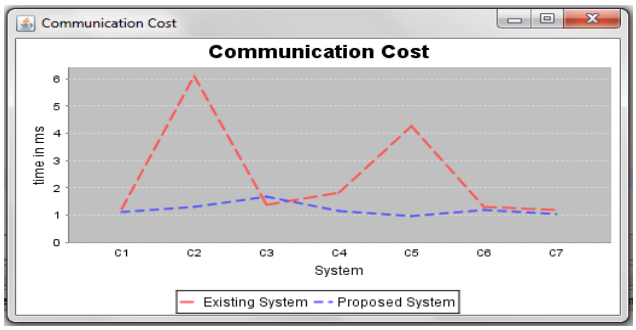


Fig 4. MR-tree node *structure*

V. RESULTS

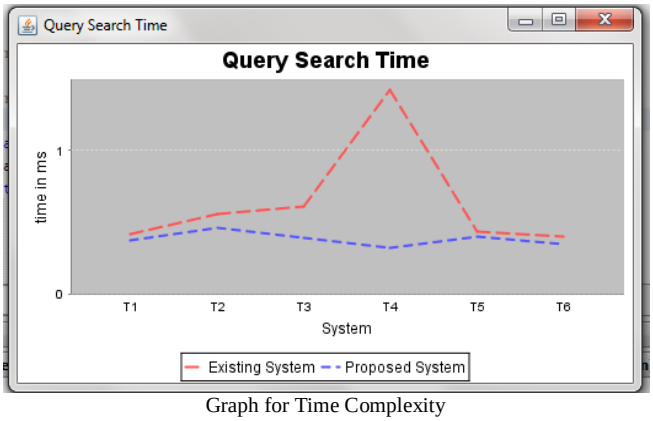
1)Communication cost



X-axis: Total Communication cost
Y-axis: Communication Cost (k bytes)

Graph shows the performance of the methods as a function of data size, when data size increases communication cost, the communication frequency between the server and the client rises. As existing system is poor in communication cost performance as compared to proposed MR tree algorithm.

2)Time Complexity



Graph for Time Complexity

Above graph shows the time comparison between two data structure, time of MR-trees and existing data structure on the datasets, As MR tree construct the tree structure with root node, so query search timing is very low as compare to existing system data structure.MR tree searches query results in tree manner. If data set is large then also MR tree algorithm takes efficient timing for searching.

VI. CONCLUSION

In this paper, the proposed a novel architecture helps to identify privacy and utility tradeoffs in LBS. The architecture has a user-centric design that delays the sharing of a location coordinate until the user has evaluated the impact of its accuracy on the service quality. The implemented architecture is an 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. In this an optimization technique is developed to reduce the communication frequency when the client communicates with server. In this paper, proposed the MR-tree, and authenticated index based on the Merkle Hash tree and the R*-tree. This method outperforms the best current solution by orders of magnitude in many important metrics such as construction cost, index size and verification overhead so conclusion is like contributions with an extensive experimental study that validates the effectiveness and efficiency of the proposed structure.

References

1. Xiang-Yang Li and Taeho Jung, "Search…Privacy-preserving Location Query Service" Department of Computer Science, Illinois Institute of Technology, Chicago, ILxli@cs.iit.edu, tjung@hawk.iit.edu
2. G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous Location-Based Queries in Distributed Mobile Systems," Proc. 16th Int'l Conf. World Wide Web, pp. 371-380, 2007.
3. Rinku Dewri, Member, IEEE, and Ramakrisha Thurime" Exploiting Service Similarity for Privacy in Location-Based Search Queries", IEEE , VOL. 25, NO. 2, Feb 2014
4. M. Duckham and L. Kulik, "A Formal Model of Obfuscation and Negotiation for Location Privacy," Proc. Third Int'l Conf. Pervasive Computing, pp. 152-170, 2005.
5. P. Golle and K. Partridge, "On the Anonymity of Home/Work Location Pairs," Proc. Seventh Int'l Conf. Pervasive Computing, pp. 390-397, 2009.
6. 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.
7. R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, "Preserving User Location Privacy in Mobile Data Management Infrastructures," Proc. Sixth Workshop Privacy Enhancing Technologies, pp. 393-412, 2006.
8. H. Zang and J. Bolot, "Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study," Proc. 17th Ann. Int'l Conf. Mobile Computing and Networking, pp. 145-156, 2011.
9. Y. Yang, S. Papadopoulos, D. Papadias, and G. Kollios. Spatial Outsourcing for Location-based Services. In ICDE, pages 1082– 1091, 2008.
10. J. Sythoff and J. Morrison, Location-Based Services: Market Forecast, 2011-2015, Pyramid Research, 2011.
11. P. Golle and K. Partridge, "On the Anonymity of Home/Work Location Pairs," Proc. Seventh Int'l Conf. Pervasive Computing, pp. 390-397, 2009.
12. F. Aurenhammer and O. Schwarzkopf, "A Simple On-line Randomized Incremental Algorithm for Computing Higher Order Voronoi Diagrams," Proc. Seventh Ann. Symp. Computational Geometry, pp. 142-151, 1991

