ISSN:2320-0790

An International Journal of Advanced Computer Technology

Location Based Queries for Content Protecting In Privacy Preserving

Dr.S.Sujatha(HOD), N.Premalatha(M.Phil Scholar)
School of information technology and science, Dr.G.R.Damodaran College of science

Abstract: Mobile devices with global positioning capabilities allow users to retrieve points of interest in their proximity. To protect user privacy, it is important not to disclose exact user coordinates to un-trusted entities that provide location-based services. Currently, there are two main approaches to protect the location privacy of users: hiding locations inside cloaking regions and encrypting location data using private information retrieval protocols. Previous work focused on finding good trade-offs between privacy and performance of user protection techniques, but disregarded the important issue of protecting the POI dataset. It is very easy for a person to know his/her location with the help of devices having GPS facility. When user's location is provided to LBS, it is possible to user to know all location dependent information like location of friends or Nearest Restaurant, whether or traffic conditions. The massive use of mobile devices pave the way for the creation of wireless networks that can be used to exchange information based on locations. When the exchange of location information is done amongst entrusted parties, the privacy of the user could be in harmful. Existing protocol doesn't work on many different mobile devices and another issue is that, Location Server (LS) should provide misleading data to user. Privacy preserving reputation techniques provides a suitable approach to address such problem. They can be easily integrated into our methods.

Keywords: Location server, overhead, private information retrieval, reputation technique, privacy.

I. INTRODUCTION

Location based service can offer many services to the users based on the geographical position of their mobile device. The services provided by LBS are typically based on a point of interest database. By retrieving the Points Of Interest (POIs) from the database server, the user can get answers to various location based queries, which include but are not limited to - discovering the nearest ATM machine, gas station, hospital, or police station. Private Information Retrieval (PIR) protocols allow a client to retrieve one bit from a database, without the server inferring any information about the queried bit. Private information retrieval (PIR) is a way for a client to look up information in an online database without letting the database servers learns the query terms or responses. The goal of PIR is to transmit less data while still protecting the privacy of the query. These protocols are too costly in practice because they invoke complex arithmetic operations for every bit of the database. Here a major enhancement introduced into two stage approach, where the first stage is based on Oblivious Transfer and the second stage is based on Private Information Retrieval (PIR), to achieve a secure solution for both parties. Here introduce a successful privacy preserving Location Based Services (LBS) must be secure and provide accurate query results. Privacy preserving Location Based Services is deal with the privacy and the accuracy issues of privacy-preserving LBS. As LBS is a developing technology, users might not be aware of the risks that it poses. New types of smart mobile devices enabled the emergence of Location-Based Services (LBS). A user of the service carries a mobile device that obtains its location via GPS or a Wireless Local Area Network (WLAN).In location based services (LBS), users with location were mobile devices can query their surroundings anywhere and at any time. While this ubiquitous computing paradigm brings great convenience for information access, it raises a concern of potential intrusion on user's location privacy, which has hampered the widespread use of LBS. Users of mobile devices tend to frequently have a need to find Points Of Interest (POIs), such as restaurants, hotels, or gas stations, in close proximity to their current locations. Collections of these POIs are typically stored in databases administered by Location Based Service (LBS) providers such as Google, Yahoo!, and

Microsoft, and are accessed by the company's own mobile client applications or are licensed to third party independent software vendors. A user first establishes his or her current position on a smartphone such as a RIM BlackBerry, Apple iPhone, or Google Android device through a positioning technology such as GPS (Global Positioning System) or cell tower triangulation, and uses it as the origin for the search. The problem is that if the user's actual location is provided as the origin to the LBS, which performs the lookup of the POIs, then the LBS will learn that location.

II. DESIGN AND REQIUREMENTS

Users of mobile devices tend to frequently have a need to find Points of Interest, such as restaurants, hotels, or gas stations, in close proximity to their current locations. Collections of these POIs are typically stored in databases administered by Location Based Service providers such as Google, Yahoo!, and Microsoft, and are accessed by the company's own mobile client applications or are licensed to third party independent software vendors. A user first establishes his or her current position on a smartphone such as a RIM BlackBerry, Apple iPhone, or Google Android device through a positioning technology such as GPS (Global Positioning System) c or cell tower triangulation, and uses it as the origin for the search. The problem is that if the user's actual location is provided as the origin to the LBS, which performs the lookup of the POIs, then the LBS will learn that location. The server encrypts each record ri within each cell of Q, Qi, j, with an associated symmetric key ki,j . The encryption keys are stored in a small (virtual) database table that associates each cell in the public grid P, Pi, j, With both a cell in the private grid Qi and corresponding symmetric key Ki, j .The server then processes the encrypted records within each cell Qi,j such that the user can use an efficient PIR,to query the records. Using the private partition Q, the server represents each associated (encrypted) data as an integer Ci, with respect to the cloaking region. For each Ci, the server chooses a set of unique prime powers $\pi i = pci\ I$, such that $Ci < \pi i$

We note that the ci in the exponent must be small forthe phase to work efficiently. Finally, the server uses the Chinese Remainder Theorem to find the smallest integer e such that $e = Ci \pmod{\pi i}$ for all Ci. The integer e effectively represents the database. Once the initialization is complete, the user can proceed to query the location server for POI records.

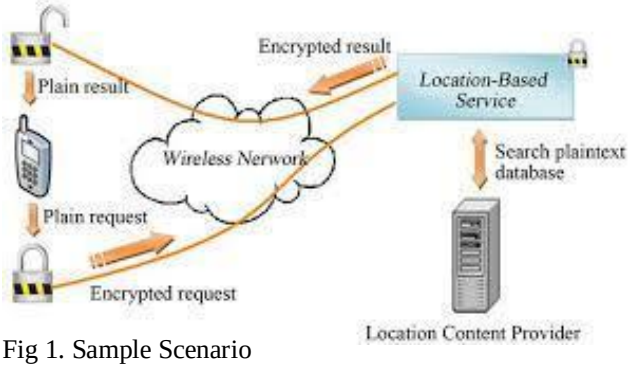


Fig 1. Sample Scenario

EXISTING SYSTEM:

In existing system the two stage approach is introduced for privacy preserving and content protecting location based queries, 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. We implement our solution on a desktop machine and a mobile device to assess the efficiency of our protocol. The mobile result we provide may be different than other mobile devices and software environments. Also, we need to reduce the overhead of the primarily test used in the private information retrieval based protocol.

DISADVANTAGE:

- Location server supplying misleading data to client.
- Overhead problem occurs in primarily test used in the private information retrieval phase.
- Incorrect conclusion may be derived.

PROPOSED SYSTEM:

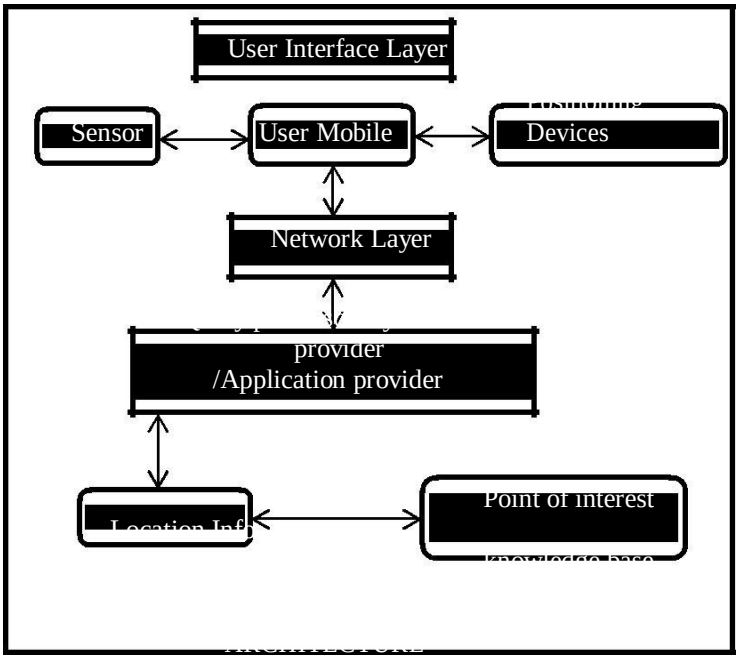
Privacy preserving reputation technique is a revolutionary paradigm in which volunteers collect and share information from their local environment using mobile phones. The design of a successful reputation technique application is met with two challenges - user privacy and data trustworthiness. In this work, we present a way to transfer reputation values which is a proxy for assessing trustworthiness between anonymous contributions. In the first step, user locations are generalized to coarse-grained CRs which provide strong privacy. Next, a PIR protocol is applied with respect to the obtained query CR. To protect excessive disclosure of POI locations, we devise a cryptographic protocol that privately evaluates whether a point is enclosed inside a rectangular region.

ADVANTAGE:

•Users are vulnerable to linking attack if they naively reveal their reputations to the application server.

•Minimize the risk of such attack.

•It can reduce the link ability



LITERATURE SURVEY:

Achieving Efficient Query Privacy for Location Based Services: We present a technique for private information retrieval that allows a user to retrieve information from a database server without revealing what is actually being retrieved from the server. We perform the retrieval operation in a computationally efficient manner to make it practical for resource-constrained hardware such as smartphones, which have limited processing power, memory, and wireless bandwidth. In particular, our algorithm makes use of a variable-sized cloaking region that increases the location privacy of the user at the cost of additional computation, but maintains the same traffic cost.
A Hybrid Technique for

Private Location-Based Queries with Database Protection:
Mobile devices with global positioning capabilities allow users to retrieve points of interest (POI) in their proximity. To protect user privacy, it is important not to disclose exact user coordinates to un-trusted entities that provide location-based services. We propose a hybrid, two-step approach to private location-based queries, which provides protection for both the users and the database. In the first step, user locations are generalized to coarse-grained CRs which provide strong privacy. Next, a PIR protocol is applied with respect to the obtained query CR. To protect excessive disclosure of POI locations, we devise a cryptographic protocol that privately evaluates whether a point is enclosed inside a rectangular region. We also introduce an algorithm to efficiently support PIR on dynamic POI sub-sets. **Achieving Efficient Query Privacy for Location Based Services:** We present a technique for private information retrieval that allows a user to retrieve information from a database server without revealing what is actually being retrieved from the server. We perform the retrieval operation in a computationally efficient manner to make it practical for resource-constrained hardware such as smartphones, which have limited processing power, memory, and wireless bandwidth. In particular, our algorithm makes use of a variable sized cloaking region that increases the location privacy of the user at the cost of additional computation, but maintains the same traffic cost.

Algorithm :Privacy preserving reputation

1: A sends around her public key K to all Bi belongs to S along with TM(A, Bi)
2: Each member of Bi computes IT E(A, Bi, x), encrypts it and sends the encrypted form C to the third party Z.
3: Z generates a random permutation of the encrypted messages and sends it to A.
4: A decrypts the messages and computes the required sum ρ(A, x).At each iteration, the algorithm will increment the variable adaptively with respect to inter and intra node buffers.

The first scheme, presented in Algorithm 1, assumes that every member Bi ∈ S knows the trust value, TM(A, Bi), that member A has in her, or that A is willing to disclose this information to Bi . It is also assumed that a partially trusted third party Z exist (i.e. Z does not collude with other agents, and she has no access to any private information of the involved parties). The encryption ensures that only Bi knows ITE(A, Bi , x). The permutation carried out by Z ensures that when the set of values ITE(A, Bi , x) is received by A, the origin of the ITE(A, Bi , x) value is not clear to A. This scheme achieves our computational goal and therefore enables private computation of reputation by any member A. Collusion between any of the members (excluding Z) in this scheme is not helpful, since they have no access to information related to non-colluding members. The main advantage of this scheme is its simplicity and small communication overhead , while its main disadvantage is the disclosure of member trust values. Although deemed otherwise, this privacy violation is not very severe: being in A's trust-set, members already know that their corresponding trust value is above the threshold α.

III. EVALUATION

After the users finished all of the test queries in the test phase, the training phase begins. The clicked results from the test phase are treated as positive training samples Q in Location training. The click through data, the extracted content concepts, and the extracted location concepts are employed in training to obtain the personalized ranking. After the training phase, the evaluation phase is performed to decide if the personalized ranking function obtained in the training phase can indeed return more relevant results for the user. Each user was asked to provide relevance judgment on all of the top results R for each query he/she has tested in the test phase by grading each result with one of the three levels of relevancy

("Relevant," "Fair," and "Irrelevant").To this end, the user scans through the full-text of the results using the preview function provided by the prototype and then gives relevance ratings to all of the results returned by the server.

GPS Locations:

We evaluate the impact of GPS locations, as defined in (2),location GPS employs only the location-based features which take into account both the location concepts and the GPS locations. The user's GPS locations and locations closely related to the GPS locations receive higher weights in the location weight vector. We observe that the lowest average relevant rank is achieved when w GPS= 0:1. When w GPS=0.1 increases beyond 0.1, the ranking quality degrades, because the ranking has a bias towards the GPS locations, while ignoring the location information extracted from the click through data.

IV. CONCLUSION

In this paper reduced the overhead of primarily test of all retrieved information in the private information retrieval phase. The accurate data is sent to the receiver without any misleading of data. For this privacy preserving reputation technique is used so that we can able to send data only for correct users. Client can retrieve the queried information accurately without any delay and that information is not known to the server. This work is implemented with different mobile and desktop devices.

V. REFERENCES

[1] C. Aguilar-Melchor and P. Gaborit. A lattice-based computationally-efficient private information retrieval protocol. Cryptology ePrint Archive, Report 2007/446, 2007.

[2] H. S.-M. Ali Khoshgozaran and C. Shahabi. SPIRAL, a scalable private information retrieval approach to location privacy. In Proceedings of the 2nd International Workshop on Privacy-Aware Location based Mobile Services (PALMS), 2008.

[3]. B. Bamba, L. Liu, P. Pesti, and T. Wang. Supporting anonymous location queries in mobile environments with privacy grid. In Proceeding of the 17th international conference on World Wide Web, pages 237–246, New York, NY, USA, 2008.

A. Beimel and Y. Stahl. Robust information-theoretic private information retrieval. J. Cryptol., 20(3):295–321, 2007.