ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
*A Peer Reviewed Open Access International Journal*

# Content Protecting and Secrecy Maintaining For Location Based Queries

**PendyalaPranay Kumar**
Department of CSE,
Arjun College of Technology & Science.

**B.Chandra Sekhar**
Assistant Professor,
Department of CSE,
Arjun College of Technology & Science.

## Abstract:

In this project, we implemented solution to location based query problem. The problem that we have gone through is stated below

(i) An End 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 do propose a major enhancement upon previous solutions through a two stage approach, where the first step is based on clear Transfer and the second step is based on Private Information Access, to achieve a secure solution for both parties. The solution we present is efficient and practical in many scenarios. The solution for the problem is implemented on a desktop machine to assess the efficiency of our protocol. We also introduce a security model and analyze 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. Along with this, we also implement text related queries, in which the end user can either search nearest objects of can search required text related queries (like search engine).

## INTRODUCTION:

ALOCATION based service (LBS) is an information,ent ertainment and utility service generally accessibleby mobile devices such as, mobile phones, GPS devices,pocket PCs, and operating through a mobile network. ALBS can offer many services to the users based on thegeographical position of their mobile device.

The servicesprovided by a LBS are typically based on a point of interestdatabase. By retrieving the Points Of Interest (POIs) fromthe database server, the user can get answers to variouslocation based queries, which include but are not limitedto - discovering the nearest ATM machine, gas station, hospital,or police station. In recent years there has been adramatic increase in the number of mobile devices queryinglocation servers for information about POIs. Among manychallenging barriers to the wide deployment of such application,privacy assurance is a major issue. For instance,users may feel reluctant to disclose their locations to theLBS, because it may be possible for a location server tolearn who is making a certain query by linking these locationswith a residential phone book database, since usersare likely to perform many queries from home.

The Location Server (LS), which offers some LBS, spendsits resources to compile information about various interestingPOIs. Hence, it is expected that the LS would not disclose any information without fees. Therefore the LBShas to ensure that LS's data is not accessed by any unauthorizeduser. During the process of transmission the usersshould not be allowed to discover any information forwhich they have not paid. It is thus crucial that solutionsbe devised that address the privacy of the users issuingqueries, but also prevent users from accessing content toswhich they do not have authorization.

## SYSTEM ANALYSIS:

### Existing System:

The Location Server (LS), which offers some LBS, spends its resources to compile information about various interesting POIs. Hence, it is expected that the LS would not disclose any information without fees. Therefore the LBS has to ensure that LS's data is not accessed by any unauthorized user. During the process of transmission the users should not be allowed to discover any information for which they have not paid.

It is thus crucial that solutions be devised that address the privacy of the users issuing queries, but also prevent users from accessing content to which they do not have authorization.

## Disadvantages of Existing System:

•Among many challenging barriers to the wide deployment of such application, privacy assurance is a major issue.
•The user can get answers to various location based queries.

## PROPOSED SYSTEM:

In this paper, we propose a novel protocol for location based queries that has major performance improvements with respect to the approach by Ghinita at el. And. Like such protocol, our protocol is organized according to two stages. In the first stage, the user privately determines his/her location within a public grid, using oblivious transfer. This data contains both the ID and associated symmetric key for the block of data in the private grid. In the second stage, the user executes a communicational efficient PIR, to retrieve the appropriate block in the private grid. This block is decrypted using the symmetric key obtained in the previous stage. Our protocol thus provides protection for both the user and the server. The user is protected because the server is unable to determine his/her location. Similarly, the server's data is protected since a malicious user can only decrypt the block of data obtained by PIR with the encryption key acquired in the previous stage. In other words, users cannot gain any more data than what they have paid for. We remark that this paper is an enhancement of a previous work.

## Extension for Proposed System:

As the extension of our system, along with the proposed system(location based queries), we also implement text related queries, in which the end user can either search nearest objects of can search required text related queries (like search engine ).

## Advantages of Proposed System

» Redesigned the key structure.
» Added a formal security model.
» Implemented the solution on desktop machine.

## LITERATURE SURVEY:

Here, in this project, we implemented solution to location based query problem. The problem that we have gone through is stated below: An End-user wants to query a database of location data, known as Points Of Interest (POIs), and does not want to reveal his/her location tithe server due to privacy concerns; 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 do propose a major enhancement upon previous solutions through a two stage approach, where the first step is based on clear Transfer and the second step is based on Private Information Access, to achieve a secure solution for both parties. The solution we present is efficient and practical in many scenarios. The solution for the problem is implemented on a desktop machine to assess the efficiency of our protocol. We also introduce a security model and analyze 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. Along with this, we also implement text related queries, in which the end user can either search nearest objects of can search required text related queries (like search engine ).

## IMPLEMENTATION

## Modules:

1.User Module
2.Admin Module
3.Application Module
4.Key Generation
5.Encryption Module

## Modules description:

### User Module:

In this module, users are able to register in our application, so that they can be allowed to access our application. To become a valid user of our application, everyone should go through registration form that is available in our application and should provide user name and password to have a valid id.

## Admin Module:

Admin module refers to Administrator of our application. An admin has the rights to activate or deactivate a particular user in order to make him to access or to reject accessing our application. If admin finds a user as fraud one of finds a user as doing illegal operations in our application, then Admin just blocks that user from accessing the application.

## Application Module:

It is a module, where end user query is transferred to map server. In our system, google map. For example we are searching for nearest temples, and then the application module sends our current location and our query (in this case, nearest temples) to the google map server.

## Key Generation:

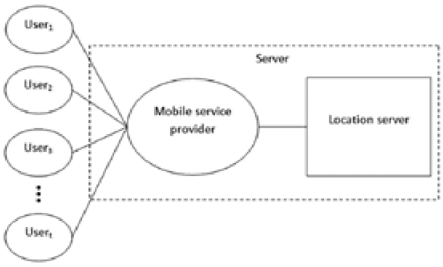
A key is generated to make a plain text into a cipher text to make our personal information secure at administrator. The encryption function accepts a generated key and user personal information as inputs and generates a cipher text.

## Encryption:

The encryption function accepts a generated key and user personal information as inputs and generates a cipher text.

## SYSTEM DESIGN:

## System Architecture:



## Data flow diagram:

1.The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

2.The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

3.DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

## 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 Ghinitaet 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 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 primality 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.

## REFERENCES:

[1] (2011, Jul. 7) Openssl[Online]. Available:http://www.openssl.org/.

[2] M. Bellare and S. Micali, "Non-interactive oblivious transfer and applications," in Proc. CRYPTO, 1990, pp. 547–557.

[3] A. Beresford and F. Stajano, "Location privacy in pervasive computing," IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, Jan.–Mar. 2003.

[4] C. Bettini, X. Wang, and S. Jajodia, "Protecting privacy against location-based personal identification," in Proc. 2nd VDLB Int. Conf. SDM, W. Jonker and M. Petkovic, Eds., Trondheim, Norway, 2005, pp. 185–199, LNCS 3674.

[5] X. Chen and J. Pang, "Measuring query privacy in location-based services," in Proc. 2nd ACM CODASPY, San Antonio, TX, USA, 2012, pp. 49–60.

[6] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," J. ACM, vol. 45, no. 6, pp. 965–981, 1998.

[7] M. Damiani, E. Bertino, and C. Silvestri, "The PROBE framework for the personalized cloaking of private locations," Trans. Data Privacy, vol. 3, no. 2, pp. 123–148, 2010.

[8] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in Proc. 3rd Int. Conf. Pervasive Comput., H. Gellersen, R. Want, and A. Schmidt, Eds., 2005, pp. 243–251, LNCS 3468.

[9] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inform. Theory, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[10] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in Proc. ICDCS, Columbus, OH, USA, 2005, pp. 620–629.

[11] C. Gentry and Z. Ramzan, "Single-database private information retrieval with constant communication rate," in Proc. ICALP, L. Caires, G. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, Eds., Lisbon, Portugal, 2005, pp. 803–815, LNCS 3580.

[12] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "A hybrid technique for private location-based queries with database protection," in Proc. Adv. Spatial Temporal Databases, N. Mamoulis, T. Seidl, T. Pedersen, K. Torp, and I. Assent, Eds., Aalborg, Denmark, 2009, pp. 98–116, LNCS 5644.

[13] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearestneighbor queries with database protection," GeoInformatica, vol. 15, no. 14, pp. 1–28, 2010.

[14] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in Proc. ACM SIGMOD, Vancouver, BC, Canada, 2008, pp. 121–132.

[15] G. Ghinita, C. R. Vicente, N. Shang, and E. Bertino, "Privacypreserving matching of spatial datasets with protection against background knowledge," in Proc. 18th SIGSPATIAL Int. Conf. GIS, 2010, pp. 3–12.