INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 5, Issue 1 SEP 2015

# Location Based Queries Using PIR Protocol

[1] Thyagarajan Chinna, [2] B.Bharath Kumar

[1]M.Tech Student, Department of CSE.

thyagacse5b1@gmail.com

[2] Assistant Professor, Department of CSE.

bandlabharathkumar@gmail.com

**ABSTRACT—**In this paper we introduce an answer for one of the area based inquiry issues. This issue is characterized as tails: (i) a client needs to question a database of area information, known as Points Of Interest (POIs), and would not like to uncover his/her area to the server because of security concerns; (ii) the proprietor of the area information, that is, the area server, would not like to just circulate its information to all clients.The area server goals to have some control over its information, since the information is its advantage. We propose a noteworthy improvement upon past arrangements by presenting a two stage approach, where the first step is in light of Oblivious Transfer and the second step is taking into account Private Information Retrieval, to accomplish a safe answer for both sides. The arrangement we present is proficient and handy in numerous situations. We actualize our answer on a desktop machine and a cell phone to survey the proficiency of our convention. We likewise present a security demonstrate and break down the security in the connection of our convention. At long last, we highlight a security shortcoming of our past work and present an answer for overcome it.

**Index Terms—**Location based question, private inquiry, private data recovery, unaware exchange.

## 1.INTRODUCTION:

A Location based administration (LBS) is a data diversion and utility administration by and large available by cell phones, for example, cellular telephones, GPS gadgets, pocket PCs, and working through a versatile system. A LBS can offer numerous administrations to the clients taking into account the land position of their cell phone. The administrations given by a LBS are ordinarily taking into account a state of hobby database. By recovering the Points Of Interest (POIs) from the database server, the client can get answers to different area based questions, which incorporate however are not restricted to - finding the closest ATM machine, corner store, doctor's facility, or police headquarters. Lately there has been a emotional increment in the quantity of cell phones questioning area servers for data about POIs.

Among numerous testing obstructions to the wide sending of such application, protection certification is a noteworthy issue. Case in point, clients may feel hestant to uncover their areas to the LBS, on the grounds that it might be workable for an area server to realize who is linking so as to make a certain inquiry these areas with a private telephone directory database, since clients are prone to perform numerous inquiries from home. The Location Server (LS), which offers a few LBS, spends its assets to accumulate data about different intriguing POIs. Consequently, it is normal that the LS would not reveal any data without expenses. Accordingly the LBS needs to guarantee that LS's information is not got to by any unapproved client. Amid the procedure of transmission the clients should not be permitted to find any data for which they have not paid. It is in this manner urgent that arrangements be contrived that address the security of the clients issuing inquiries, additionally keep clients from getting to substance to which they don't have approval.

## 2.RELATED WORK:

The main answer for the issue was proposed by Beresford , in which the security of the client is kept up by always showing signs of change the client's name or pen name inside of some blend zone. It can be demonstrated that, because of the nature of the information being traded between the client and the server, the regular changing of the client's name gives little security to the client's protection. A later examination of the blend zone methodology has been connected to street systems . They examined the obliged number of clients to fulfill the unlinkability property when there are rehashed inquiries over an interim. This obliges watchful control of what number of clients are contained inside of the blend zone, which is hard to accomplish by and by.

A corresponding strategy to the blend zone approach is in view of k-secrecy . The idea of k-secrecy was presented as a system for protecting security when discharging delicate records.This is accomplished by speculation and concealment calculations to guarantee that a record couldn't be recognized from $(k-1)$ different records. The answers for LBS utilize a trusted anonymiser to give namelessness to the area information, such that the area information of a client can't be recognized from $(k-1)$ different clients.

An improved trusted anonymiser methodology has likewise been proposed, which permits the clients to set their level of security in light of the estimation of k. This implies that, given the overhead of the anonymiser, a little estimation of k could be utilized to build the effectiveness. On the other hand, a expansive estimation of k could be decided to enhance the security, on the off chance that the clients felt that their position information could be utilized perniciously. Picking a worth for k, be that as it may, appears to be unnatural.

There have been endeavors to make the procedure less simulated by including the idea of feeling-based security . Rather than indicating a k, they suggest that the client indicates a shrouding area that they feel will secure their security, and the framework sets the quantity of cells for the locale in view of the notoriety of the region. The ubiquity is figured by utilizing verifiable foot shaped impression database that the server gathered.

New security measurements have been recommended that catches the clients' security as for LBSs . The creators start by investigating the deficiencies of straightforward k-namelessness in the setting of area questions. Next, they propose security measurements that empowers the clients to indicate values that better match their question security necessities. From these protection measurements they additionally propose spatial speculation calculations that agree with the client's security necessities.

Strategies have additionally been proposed to confound and mutilate the area information, which incorporate way and position disarray. Way disarray was introduced by Hoh and Gruteser. The essential thought is to add instability to the area information of the clients at the focuses the ways of the clients cross, making it difficult to follow clients in light of crude area information that was k-anonymised. Position disarray has additionally been proposed as a way to deal with give security . The thought is for the trusted anonymiser to gather the clients agreeing to a shrouding area (CR), therefore making it harder for the LS to distinguish a person. A typical issue with general CR procedures is that there may exist some semantic data about the geology of an area that gives away the client's area. Case in point, it would not bode well for a client to be on the water without some sort of watercraft.

Additionally, distinctive individuals may discover certain spots delicate. Damiani et al. have exhibited a structure that comprises of a jumbling motor that takes a clients profile, which contains places that the client esteems touchy, and yields jumbled areas in light of conglomerating calculat

## 3.SYSTEM MODEL:

The framework model comprises of three sorts of substances (see Fig. 1): the arrangement of users1 who wish to get to area information U, a versatile administration supplier SP, and an area server LS. From the perspective of a client, the SP and LS will create a server, which will serve both capacities. The client does not should be concerned with the specifics of the correspondence.

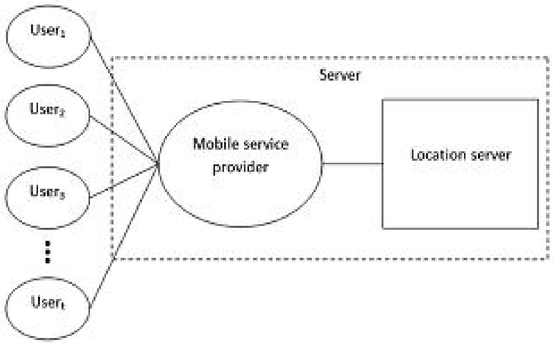


Fig. 1. System model.

The clients in our model utilize some area based administration given by the area server LS. Case in point, what is the closest ATM or eatery? The motivation behind the versatile administration supplier SP is to build up and keep up the correspondence between the area server and the client. The area server LS claims an arrangement of POI records ri for 1 ≤ ri ≤ ρ.

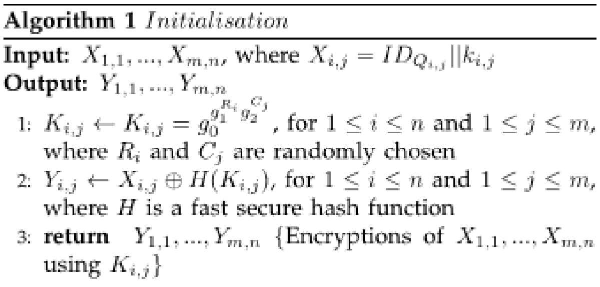
Every record depicts a POI, giving GPS directions to its area (xgps, ygps), and a depiction or name about what is at the area. We sensibly expect that the versatile administration supplier SP is an aloof substance and is not permitted to connive with the LS. We make this presumption in light of the fact that the SP can focus the whereabouts of a cell phone, which, if permitted to conspire with the LS, totally subverts any strategy for protection. There is basically no innovative strategy for keeping this assault. As a result of this supposition, the client has the capacity either utilize GPS (Global Positioning Framework) or the versatile administration supplier to obtain his/her coordinates.

Since we are expecting that the versatile administration supplier SP is trusted to keep up the association, we consider just two conceivable enemies. One for every correspondence bearing. We consider the case in which the client is the enemy and tries to get more than he/she is permitted. Next we consider the case in which the area server LS is the enemy, and tries to exceptionally relate a client with a framework coordinate.

**4. PROTOCOL DESCRIPTION:**

A definitive objective of our convention is to get a situated (piece) of POI records from the LS, which are near the client's position, without trading off the protection of the client or the information put away at the server. We accomplish this by applying a two stage methodology indicated in Fig. 2. The principal stage is taking into account a two-dimensional unaware exchange and the second stage is taking into account a communicationally effective PIR . The unmindful exchange based convention is utilized by the client to get the cell ID, where the client is found, and the comparing symmetric key. The learning of the cell ID and the symmetric key is then utilized as a part of the PIR based convention to acquire and unscramble the area information.

The client decides his/her area inside of an openly produced matrix P by utilizing his/her GPS coordinates and frames a neglectful exchange query2. The base measurements of the general population framework are characterized by the server and are made accessible to all clients of the framework. This open network superimposes over the secretly parceled framework created by the area server's POI records, such that for every cell Qi, j in the server's parcel there is no less than one Pi, j cell from people in general framework. This is delineated in Fig. 3. Since PIR does not oblige that a client is compelled to acquire one and only bit/obstruct, the area server needs to actualize some assurance for its records. This is accomplished by scrambling every record in the POI database with a key utilizing a symmetric key calculation, where the key for encryption is the same key utilized for unscrambling. This key is enlarged with the cell information recovered by the unaware exchange question.



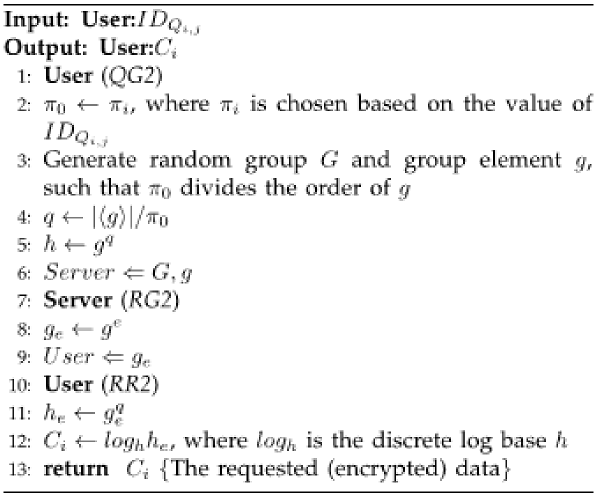
```
Algorithm 1 Initialisation
Input: $X_{1,1}, \ldots, X_{m,n}$, where $X_{i,j} = ID_{Q_{i,j}} || k_{i,j}$
Output: $Y_{1,1}, \ldots, Y_{m,n}$
  1: $K_{i,j} \leftarrow K_{i,j} = g_0^{g_1^{R_i} g_2^{C_j}}$, for $1 \leq i \leq n$ and $1 \leq j \leq m$,
     where $R_i$ and $C_j$ are randomly chosen
  2: $Y_{i,j} \leftarrow X_{i,j} \oplus H(K_{i,j})$, for $1 \leq i \leq n$ and $1 \leq j \leq m$,
     where $H$ is a fast secure hash function
  3: return $Y_{1,1}, \ldots, Y_{m,n}$ {Encryptions of $X_{1,1}, \ldots, X_{m,n}$
     using $K_{i,j}$}
```

A client u from the arrangement of clients U starts the convention process by choosing a suitable square shrouding district CR, which contains the area. All client inquiries will be as for this shrouding locale. The client likewise chooses on the exactness of this shrouding locale by what number of cells are contained inside of it, whose size can't be littler than the base size characterized by the area server. which is at any rate the base size characterized by the server. This data is joined with the measurements of the CR to structure people in general lattice P and submitted to the area server, which segments its records or superimposes it over prepartitioned records (see Fig. 3).

This segment is meant Q (note that the cells don't fundamentally should be the same size as the cells of P). Every cell in the parcel Q must have the same number rmax of POI records. Any variety in this number could prompt the server recognizing the client. In the event that this requirement can't be fulfilled, then sham records can be used to verify every cell has the same measure of information. We accept that the LS does not populate the private lattice with misdirecting or off base information, since such activity would result in the loss of business under an installment model.

Next, the server scrambles every record ri inside of every cell of Q, Qi, j, with a related symmetric key ki, j. The encryption keys are put away in a little (virtual) database table that partners every cell in the general population matrix P, Pi, j, with both a cell in the private network Qi, j and relating symmetric key ki, j.

**Algorithm 2**: PIR PROTOCOL.



```
Input: User:$ID_{Q_{i,j}}$
Output: User:$C_i$
User ($QG2$)
$\pi_0 \leftarrow \pi_i$, where $\pi_i$ is chosen based on the value of
$ID_{Q_{i,j}}$
Generate random group $G$ and group element $g$,
such that $\pi_0$ divides the order of $g$
$q \leftarrow |\langle g \rangle| / \pi_0$
$h \leftarrow g^q$
$Server \Leftarrow G, g$
Server ($RG2$)
$g_e \leftarrow g^e$
$User \Leftarrow g_e$
User ($RR2$)
$h_e \leftarrow g_e^q$
$C_i \leftarrow log_h h_e$, where $log_h$ is the discrete log base $h$
return $C_i$ {The requested (encrypted) data}
```

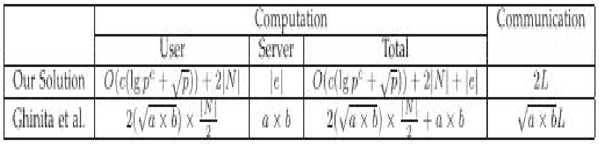
With the learning about which cells are contained in the private framework, and the information of the key that scrambles the information in the cell, the client can start a private data recovery convention with the area server to obtain the encoded POI information. Accepting the server has initialised the number e, the client ui and LS can take part in the accompanying private data recovery convention utilizing the IDQi, j, gotten from the execution of the past convention, as information. The IDQi, j permits the client to pick the related prime number force πi, which thus permits the client to inquiry the server.

## 5 EXPERIMENTS

### 5.1 Experimental Results:

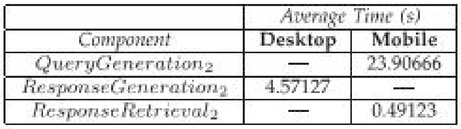
We actualized our area construct question arrangement in light of a stage comprising of: a desktop machine, running the server programming of our conventions; and a cellular telephone, running the customer programming of our conventions. For both stages, we gauged the obliged time for the neglectful exchange and private data recovery conventions independently to test the execution of every convention and the relative execution between the two conventions. The desktop machine that was utilized as a part of the analysis is prepared with an Intel Core 2 Duo E8200 2.66GHz processor and 2GB of RAM. The execution on this stage was composed utilizing Visual C++ under the Windows XP working framework. We utilized the Number Theory Library (NTL) for calculations obliging substantial numbers and OpenSSL to figure the SHA-1 hash.

Stage 2 Performance Analysis Summary



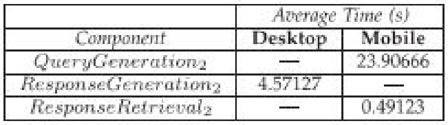
| | Computation | | | Communication |
|---|---|---|---|---|
| | User | Server | Total | |
| Our Solution | $O(c(\lg p^c + \sqrt{p})) + 2\lvert N\rvert$ | $\lvert c\rvert$ | $O(c(\lg p^c + \sqrt{p})) + 2\lvert N\rvert + \lvert c\rvert$ | $2L$ |
| Ghinita et al. | $2(\sqrt{a \times b}) \times \frac{\lvert N\rvert}{2}$ | $a \times b$ | $2(\sqrt{a \times b}) \times \frac{\lvert N\rvert}{2} + a \times b$ | $\sqrt{a \times b}L$ |

Oblivious Transfer Experimental Results for Desktop and Mobile Platforms



| | Average Time (s) | |
|---|---|---|
| Component | Desktop | Mobile |
| $QueryGeneration_2$ | — | 23.90666 |
| $ResponseGeneration_2$ | 4.57127 | — |
| $ResponseRetrieval_2$ | — | 0.49123 |

Private Information Retrieval Experimental Results for Desktop and Mobile Platforms



| | Average Time (s) | |
|---|---|---|
| Component | Desktop | Mobile |
| $QueryGeneration_2$ | — | 23.90666 |
| $ResponseGeneration_2$ | 4.57127 | — |
| $ResponseRetrieval_2$ | — | 0.49123 |

In both periods of our answer, there are 3 noteworthy steps: the client's inquiry, the server's reaction, and the client deciphering. Table 3 shows the normal runtime on the desktop what's more, versatile stages, for every part of the neglectful exchange stage. Also shows the normal times for every segment of the private data recovery convention.

When we contrast this result and our past result , we find that the convention is still functional. For this examination, we consider the execution of the customer the most imperative, since we expect that a server is effective. Contrasted and the past work, the first stage on the customer side is 4-7 times quicker, while in the second stage the customer side is 2 times slower. We must remember that the customer side was actualized on a desktop machine in the past work, and henceforth made the second stage slower. Additionally, we supplanted the hash calculation with an exponentiation operation that diminished the gathering space for gRigCj from 1024 to 160 bits. This security of this structure was secured by an external gathering of 1024 bits. Since the customer can't specifically get to gRigCj, since the discrete logarithm is hard in the external gathering, the customer must work in the external gathering to uproot the blinding components. This added to speedier execution in the first stage.

## 6.CONCLUSION

In this paper we have introduced an area based inquiry arrangement that utilizes two conventions that empowers a client to secretly focus and procure area information. The primary step is for a client to secretly focus his/her area utilizing absent exchange on an open matrix. The second step includes a private data recovery connection that recovers the record with high correspondence productivity. We dissected the execution of our convention and found it to be both computationally and communicationally more productive than the arrangement by Ghinita et al., which is the latest arrangement. We actualized a product model utilizing a desktop machine and a cell phone. The product model shows that our convention is inside down to earth limits.

Future work will include testing the convention on numerous diverse cell phones. The versatile result we give may be unique in relation to other cell phones and programming situations. Additionally, we have to diminish the overhead of the primality test utilized as a part of the private data recovery based convention. Furthermore, the issue concerning the LS supplying deceiving information to the customer is likewise intriguing. Protection saving notoriety systems appear a suitable way to deal with location such issue. A conceivable arrangement could coordinate strategies . Once suitable solid arrangements exist for the general case, they can be effortlessly incorporated into our methodology.

## 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 bfuscation 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.