Volume 6, Issue 7, July 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Resolving Location Based Queries by Providing Security to Sensitive User Data

**T. S. Ammajan**
(M.Tech) Dept of CSE,
SKUCET, SK University
Anantapur, Andhra Pradesh, India

**U. Dhanunjaya**
Assistant Professor, Dept of CSE
SKUCET, SK University
Anantapur, Andhra Pradesh, India

***Abstract:-In this paper we tend to blessing a response to 1 of the area based inquiry issues. This drawback is sketched out as tails: (i) a client needs to scrutinize a data of area data, called Points Of Interest (POIs) and doesn't have to uncover his/her area to the server on account of protection concerns; (ii) the proprietor of the position data, that is, the arrangement server, doesn't have to effectively disseminate its information to all or any clients. the arrangement server wishes to have some administration over its data, since the data is its in addition to. we tend to propose a genuine upgrade upon past arrangements by presenting a 2 phase approach, wherever the essential stride is predicated on Oblivious Transfer and the second step is predicated on non-open information Retrieval, to understand a protected determination for every gatherings. the answer we tend to blessing is proficient and sensible in a few inevitabilities. we tend to actualize our determination on a desktop machine and a cell phone to evaluate the proficiency of our protocol. we tend to conjointly present a security display and break down the wellbeing inside the context of such protocol. In conclusion, we indicate a security disadvantage of the past work we did and blessing a response to beat it.***

***Keywords: LBS, PIR, GPS, POI***

## I. INTRODUCTON

Location based mostly service (LBS) is associate degree info, entertainment and utility service typically accessible by mobile devices like, mobile phones, GPS devices, pocket PCs, and in operation through a mobile network. A LBS offers several services to the clients upheld the geographical position of their mobile gadget. The services gave by a LBS ar usually upheld a level of interest database. By retrieving the Points Of Interest (POIs) from the information server, the client will motivate answers to varied location based mostly inquiries, that typify however don't appear to be limited to - discovering the nearest ATM machine, petrol station, hospital, or station. As of late there has been a dramatic increase within the range of mobile devices querying location servers for info regarding POIs. Among many challenging barriers to the wide preparation of such aplication, privacy assurance may be a major issue. for example, clients may feel reluctant to unveil their locations to the LBS, as a consequence of it ought to be doable for a location server to learn United Nations agency is creating a definite inquiry by linking these locations with a residential telephone directory information, since clients are without a doubt to play out several questions from home. The Location Server (LS), that offers a few LBS, spends its resources to assemble data regarding varied fascinating POIs. Subsequently, it's normal that the LS wouldn't reveal any data while not charges. So the LBS has to make beyond any doubt that LS's information isn't accessed by any unauthorized client. Throughout the technique for transmission the clients ought not be allowed to find any data for which they require not paid. it's crucial to the point that arrangements be contrived that address the privacy of the clients issue questions, however additionally forestall clients from accessing substance to which they are doing not have authorization. The ultimate goal of our protocol is to get a gathering (square) of dish records from the LS, that ar near the client's position, while not compromising the privacy of the client or the data keep at the server the first costly operation in our protocol is that the modular operation, we have an inclination to target minimizing the quantity of times it's required. we have a propensity to assume that some parts can be recomputed, and thence we have an inclination to exclusively take into account the computations required at runtime we have an inclination to analyzed the performance of our protocol and located it to be each computationally and communicational additional productive than the answer by Ghinita et al., that will be that the latest determination. we have a propensity to upheld a code model using a desktop machine and a mobile gadget. The code model demonstrates that our protocol is at intervals sensible breaking points. the location server, doesn't have to easily convey its information to any or all clients. the placement server wishes to claim some management over its information, since the info is its in addition to. Past arrangements have utilized a beyond any doubt anon miser to deal with privacy, however introduced the inutility of trusting an outsider. more modern arrangements have utilized homomorphism cryptography to dispose of such weakness. Mainly, the client submits ones coordinates those are scrambled to the server and therefore the server would confirm the client's location homomorphically, so the client would acquire the corresponding record victimization personal info Retrieval procedures. we have an inclination to propose a significant change upon this outcome by introducing an identical 2 stage approach,

 

wherever the homomorphism comparison step is replaced with Oblivious Transfer to attain a safer determination for each parties. the answer we have an inclination to blessing is economical and sensible in several eventualities. we have a propensity to conjointly typify the consequences of an operating encapsulation for instance the potency of our protocol.

## II. LITERATURE SURVEY

M. Bellare and S. Micali [2]. They are proposed a customer and fair proto col for secure two-party computation in the Optimistic model, in which a partially trusted outsider T is available, however not in volved in normal executions of protocol. T is required just if there exist disturbance in communication or on the off chance that one Of the two parties denies or misbehaves. This protocol guarantees that regardless of the fact that one party terminates the protocol at any of the time, the computation is still fair for the second party Communication is over an asynchronous network. All protocols we are using are based on customer proofs of information and involve no general zero-learning to ols as intermediate strides we portray e±cientveriø-able absent transfer. A. Beresford and F. Stajano[3] they are proposed an As location-aware applications begin to track our developments in the name of accommodation, by what method can we secure our rivacy? This article introduces the blend zone another development inspired by anonymous communication strategies together with measurements for assessing anonymity of a client which is based on nom de plumes are every now and again changing. C. Bettini, X. Wang, and S. Jajodia[4] They proposed a manuscript and we introduce an answer for one of the location predicated question quandaries. This quandary is defined as tails: (i) an utilizer wants to inquiry a database of location data, kenned as Points Of Interest (POIs) and does not optate to reveal his/her location to the server because of privacy concerns; (ii) the proprietor of the location data, that is, the location server, does not optate to just circulate its data to all the clients. Here the location server wishes to have some control over its data, since the data is its asset. We suggest a major enhancement upon anterior arrangements by introducing a two stage approach, where the initial step is predicated on Oblivious Transfer and the second step is predicated on Private Information Retrieval (PIR), to achieve a secured answer for both the parties. The arrangement which we present is entirely productive and more practical in many of the scenarios. We then execute our answer onto a desktop machine and a mobile contrivance to assess the proficiency of our protocol. We additionally introduce a security display and analyze the security in the context of our protocol. Finally, we highlight a security impotency of our atecedent work and present an answer for surmount it. X. Chen and J. Pang[5] They proposed a Vehicular networks are imagined to play an important part in the building of intelligent transportation frameworks. Be that as it may, the dangers of the remote transmission of potentially exploitable information such as detailed locations are often ignored or just inadequately addressed in field operational tests or endeavors of standardization. The main reasons for this is that the idea of privacy is hard to quantify. While vehicular network algorithms are usually evaluated by means of simulation, it is a non-trivial task to assess the performance of a privacy security mechanism. In this paper we talk about the principles, all the challenges, and also the necessary strides regarding privacy assessment in vehicular N/Ws. We also distinguish all valuable and the practical measurements that allow the comparison and evaluation of privacy assurance algo's. We thusly introduce an exceptionally systematic literature audit that reveals insight into the flow state of the art and give recommendations for future research bearings in the field. B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan[6] the proposed a study the thought of Single-Database Private Information Retrieval (PIR). The primary Single-Database PIR was developed in 1997 by Kushilevitz and Ostrovsky and since then Single-Database PIR has risen as an important primitives of cryptography. For ex., Single-Dbase PIR ended up being intimately associated with collisionresistant hash works, the neglectful transfer and also open key encryptions with some additional properties. Here in this review, we state an outline of many of the developments for Single-Database PIR (including an abstract development based upon homomorphic encryption) and portray a portion of the associations of PIR to other primitives. T. ElGamal[9] proposed another signature plan, together with the implementation of the Diffie-Hellman open key circulation plot that achieves an open key cryptosystems. The secureness of the both frameworks depends on the trouble of computing discrete logarithms over finite fields. B. Gedik and L. Liu[10] they are proposed an answer for one of the location predicated question quandaries. This quandary is defined as tails: (i) an utilizer wants to question a database of location data, kenned as Points Of Interest (POIs) and does not optate to reveal his/her location to the server because of privacy concerns; (ii) the proprietor of the location data, that is, the location server, does not optate to just convey its data to all the clients. Here the location server wishes to have some control over its data, since the data is its asset. We suggest a major enhancement upon anterior arrangements by introducing a two stage approach, where the initial step is predicated on Oblivious Transfer and the second step is predicated on Private Information Retrieval, in order to achieve an extremely secure answer for both the parties. The arrangement which we present is excessively proficient and practical in the majority of the scenarios. We then actualize our answer for/on a desktop machine and a mobile contrivance to assess the productivity of our protocol. We additionally introduce a security display and analyze the security in the context of our protocol. Finally, we highlight a security impotency of our atecedent work and present an answer for surmount it.

## III. DESIGN AND REQIUREMENTS

Clients of mobile devices tend to much of the time have a need to find Points of Interest, such as restaurants, lodgings, or gas stations, in close vicinity to their present locations. Accumulations of these POIs are typically put away in databases administered by Location Based Service suppliers such as Google, Yahoo!, and Microsoft, and are accessed by the company's own particular mobile customer applications or are authorized to outsider independent software sellers. A client first establishes his or her momentum position on a smartphone such as a RIM BlackBerry, Apple iPhone, or Google Android gadget through a positioning innovation such as GPS (Global Positioning System) c or cell tower

 

triangulation, and utilizations it as the origin for the search. The issue is that if the client's actual location is given as the origin to the LBS, which plays out the lookup of the POIs, then the LBS will learn that location. The server scrambles each record ri within each cell of Q, Qi, j, with an associated symmetric key ki,j . The encryption keys are put away in a small (virtual) database table that associates each cell in people in general lattice P, Pi, j, With both a cell in the private framework Qi and corresponding symmetric key Ki, j .The server then procedures the encoded records within each cell Qi,j such that the client can utilize a productive PIR,to inquiry the records. Using the private partition Q, the server speaks to each associated (encoded) data as an integer Ci, concerning the cloaking locale. For each Ci, the server picks an arrangement of remarkable prime forces πi= pci I, such that Ci < πiWe take note of that the ci in the type must be small forthe phase to work effectively. Finally, the server utilizes the Chinese Remainder Theorem to find the smallest integer e such that e = Ci (mod πi) for all Ci. The integer e viably speaks to the database. Once the initialization is finished, the client can continue to question the location server for POI records

## IV. 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**.**

## V. PROPOSED SYSTEM

In this framework we involve testing the protocol on several diverse mobile devices. The mobile result we offer may be totally unique in relation to alternative mobile devices and PC code situations. Also, we'd like to curtail the overhead of the property take a gander at used in the personal info retrieval based protocol. in addition, the matter regarding the L.S supply beguiling information to the purchaser is additionally attention-grabbing. Privacy defensive name systems appear a suitable approach to deal with such drawback. A conceivable arrangement may integrate strategies. Once appropriate solid arrangements exist for the overall case, they'll be basically integrated into our approach.

This algorithm utilizes the location indexes of the clients and various parallel threads to search and select rapidly all the candidate anonymous sets with more clients and their location information with more uniform conveyance to accelerate the execution of the temporal-spatial anonymous operations, and it allows the clients to design their specially crafted privacy-preserving location question demands.

Privacy preserving reputation strategy is a revolutionary paradigm in which volunteers gather and share information from their local surroundings using mobile phones. The configuration of an effective reputation method application is met with two challenges - client privacy and data trustworthiness. In this work, we introduce a way to transfer reputation values which is an intermediary for assessing trustworthiness between anonymous commitments. In the initial step, client locations are generalized to coarse-grained CRs which give solid privacy. Next, a PIR protocol is applied concerning the obtained inquiry CR. To ensure extreme revelation of POI locations, we devise a cryptographic protocol that privately evaluates whether a point is encased inside a rectangular district.

**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

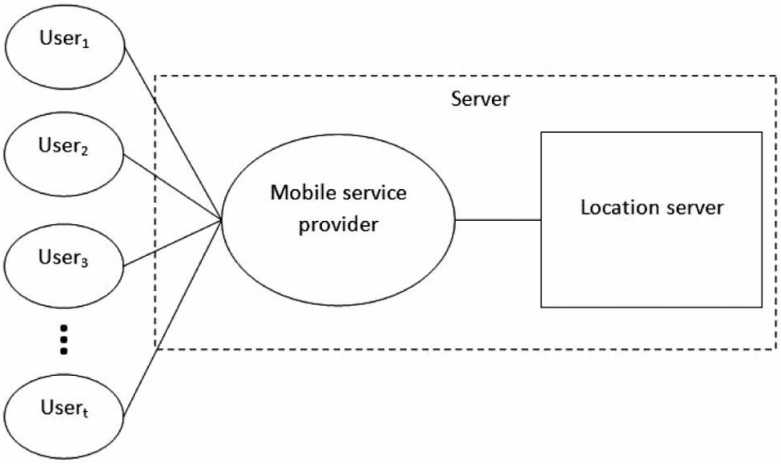


Fig. 1. System model.

 

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

Before describing our protocol we introduce the framework model, which defines the major substances and their parts. The portrayal of the protocol model begins with the notations and framework parameters of our answer.

In this paper, we propose a novel protocol for location based inquiries that has major performance upgrades as for the approach by Ghinita at el. And. Like such protocol, our protocol is organized according to two stages. In the principal stage, the client privately determines his/her location within an open lattice, using careless transfer. This data contains both the ID and associated symmetric key for the piece of data in the private framework. In the second stage, the client executes a communicational effective PIR, to recover the appropriate piece in the private lattice. This square is decoded using the symmetric key obtained in the past stage.

Our protocol hence gives security to both the client and the server. The client is ensured because the server is unable to determine his/her location. Similarly, the server's data is ensured since a malicious client can just unscramble the square of data obtained by PIR with the encryption key acquired in the past stage. In other words, clients cannot gain any a greater number of data than what they have paid for. We remark that this paper is an enhancement of a past work.

The framework model comprises of three sorts of substances (see Fig. 1): the arrangement of users1 who wish to access location data U, a mobile service supplier SP, and a location server LS. From the point of perspective of a client, the SP and LS will make a server, which will serve both capacities. The client does not should be worried with the specifics of the communication. The clients in our model utilize some location-based service gave by the location server LS. For example, what is 1. In this paper we utilize the expression "client" to allude to the element issuing inquiries and retrieving inquiry results. In many cases, such client is a customer software executing on behalf of a human client. the nearest ATM or restaurant? The motivation behind the mobile service supplier SP is to establish and maintain the communication between the location server and the client. The location server LS possesses an arrangement of POI records ri for $1 \leq ri \leq \rho$. Each record portrays a POI, giving GPS coordinates to its location (xgps, ygps), and a depiction or name about what is at the location. We reasonably assume that the mobile service supplier SP is a passive element and is not allowed to plot with the LS. We make this assumption because the SP can determine the whereabouts of a mobile gadget, which, if allowed to plot with the LS, totally subverts any strategy for privacy. There is just no technological strategy for preventing this attack. As a result of this assumption, the client can either utilize GPS (Global Positioning System) or the mobile service supplier to acquire his/her coordinates. Since we are assuming that the mobile service providerSP is trusted to maintain the association, we consider just two conceivable adversaries. One for each communication heading. We consider the case in which the client is the adversary and tries to obtain more than he/she is allowed. Next we consider the case in which the location server LS is the adversary, and tries to exceptionally associate a client with a lattice coordinate.

By studying above research works by scholar we are going to enhance this framework. Because each time client needs to determine his location and according to that he fires question to the server. So there are unnecessary strides to done to acquire piece of data from database server. So we are going to propose framework with number of clients in same open matrix or locale will acquire database using a single point. In existing framework, client inquiry to server for his NN, then server send back POI regarding to its location. Fig.5-LBS Services Using Centroid. Here we have taken into account an idea of centroid i.e. in a particular locale, there are number of obscure clients use location based services. So for each client, he has to determine his location and send it to server. So we concluded that we can make single point in the locale for communication with server .So there is no compelling reason to each client to determine its district all the time. The idea of CENTROID is not quite the same as past existing frameworks. Here we assume that, all the clients in an open framework known not other i.e. they are trusted with each other. Then one of the gatherings from general society framework can make a centroid point for communication with server because they have a trust on each other. So one of the trusted client in the gathering gain locations of other client and make a centroid point After computing the centroid, client sends it to all his companion and LBS supplier. So actual position of the client and his companions remains covered up. By getting centroid all the clients fires the inquiry regarding to that inside point. Here we cannot search nearest neighbors question .But client can access data from server from their real location and LBS server wouldn't know actual position of client and it will send data to centroid. One advantage in that is we can take predetermined number of clients from an open network. All the clients are trusted and known not other. So privacy is increases. Also we are going to enhance this by masking the locations of client and their companions while making a centroid.

## VI. SECURITY MODEL

Before we define the security of our protocol, we introduce the idea of k out of N adaptive unaware transfer as takes after. Definition 1 :( k out of N adaptive negligent transfer k×1) (OTN k×1 protocols contain two phases, for initialization and for transfer. The initialization phase is controlled by the sender (Bob) who possesses the N data components X1, X2,..., XN. Weave typically processes a promise to each of the N data components, with a total overhead of O(N). He then sends the responsibilities to the recipient (Alice). The transfer phase is utilized to transmit a single data component to Alice. At the beginning of each transfer, Alice has an input I, and her yield at the end of the phase ought to be data

 

component XI. An OTN bolsters up to k progressive transfer phases. Based on the above definition, our protocol is made out of initialization phase and transfer phase. We will now out-line the strides required for the phases and then we will formally define the security of these phases. Our transfer phase is built using six algorithms: QG1, RG1, RR1, QG2, RG2, and RR2. The initial three make the main phase (Oblivious Transfer Phase), while the last three form the second phase (Private Information Retrieval Phase). The following six algorithms are executed sequentially and are formally portrayed as takes after

**Oblivious Transfer Phase**

1) QueryGeneration1 (Client) (QG1): Takes as input indices i, j, and the dimensions of the key matrix m, n, and outputs a query Q1 and secret s1, denoted as (Q1, s1) = QG1 (i, j, m, n).
2) SResponseGeneration1 (Server) (RG1): Takes as input the key matrix Km×n, and the query Q1, and outputs a response R1, denoted as (R1)=RG1(Km×n, Q1).
3) ResponseRetrieval1 (Client) (RR1): Takes as input indices i, j, the dimensions of the key matrix m, n, the query Q1 and the secret s1, and the response R1, and outputs a cell-key ki,j and cell-id IDi,j, denoted as (ki,j,IDi,j) =RR1(i, j, m, n, (Q1,s1), R1).

**Private Information Retrieval Phase**

4) QueryGeneration2(Client)(QG2): Takes as input the cell-id IDi,j, and the set of prime powers S, and outputs a query Q2 and secret s2, denoted as (Q2,s2) = QG2(IDi,j, S).
5) ResponseGeneration2(Server)(RG2): Takes as input the database D, the query Q2, and the set of prime powers S, and outputs a response R2, denoted as (R2) = RG2(D, Q2, S).
6) ResponseRetrieval2(Client)(RR2): Takes as input the cell-key ki,j and cell-id IDi,j, the query Q2 and secret s2, the response R2,and outputs the data d, denoted as (d) =RR2(ki,j,IDi,j, (Q2,s2), R2). Our transfer phase can be repeatedly used to retrieve points of interest from the location database. With these functions described, we can build security definitions for both the client and server

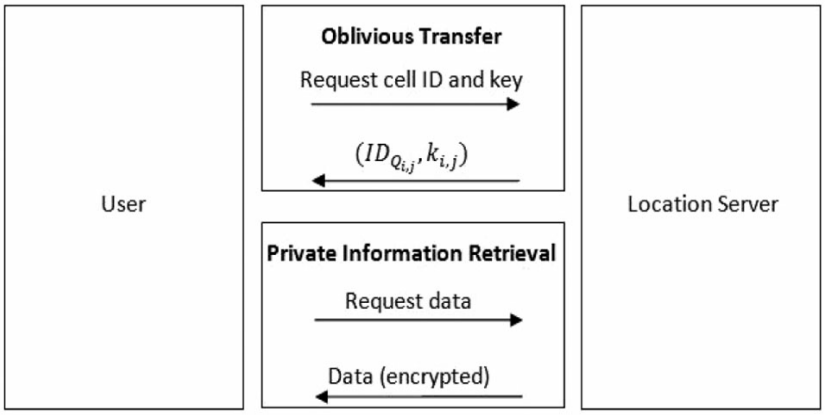


Fig. 2. High level overview of the protocol.

## VII. PROTOCOL DESCRIPTIONS

Protocol Summary The ultimate goal of our protocol is to obtain a set (square) of POI records from the LS, which are near the client's position, without compromising the privacy of the client or the data put away at the server. We achieve this by applying a two-stage approach appeared in Fig. 2. The main stage is based on a two-dimensional unmindful transfer [4] and the second stage is based on a communicationally productive PIR [7]. The client to obtain the cell ID, where the client is located, and the corresponding symmetric key utilize the absent transfer based protocol. The information of the cell ID and the symmetric key is then utilized as a part of the PIR based protocol to obtain and decode the location data. The client determines his/her location within an openly generated network P by using his/her GPS coordinates and structures a careless transfer query2. The minimum measurements of the general population network are defined by the server and are made available to all clients of the framework. This open matrix superimposes over the privately partitioned framework generated by the location server's POI records, such that for each cell Qi,j in the server's partition there is at least one Pi,j cell from people in general network. This is illustrated in Fig. 3. Since PIR does not require that a client is constrained to obtain stand out piece/obstruct, the location server needs to execute some assurance for its records. This is achieved by encrypting each record in the POI database with a key using a symmetric key algorithm, where the key for encryption is the same key utilized for decoding. This key is augmented with the cell info data recovered by the absent transfer inquiry. Subsequently, regardless of the fact that the client utilizes PIR to obtain more than one record, the data will be meaningless resulting in enhanced security for the server's database. Before we portray the protocol in detail, we depict some initialization performed by both parties and the key is send to the client side over the HMAC and MD5 alogorithms.2. An absent transfer inquiry is such that a server cannot learn the client's question, while the client cannot gain more than they are entitled. This is similar to PIR, however absent transfer requires security for the client and server. PIR just requires that the client is secured. Initialization A client u from the arrangement of clients U initiates the protocol procedure by deciding a suitable square cloaking area CR, which contains

 

his/her location. All client questions will be as for this cloaking locale. The client also settles on the accuracy of this cloaking area by what number of cells are contained within it, whose size cannot be smaller than the minimum size defined by the location server. Which is at least the minimum size defined by the server? This information is combined with the measurements of the CR to frame people in general lattice P and submitted to the location server, which partitions its records or superimposes it over repartitioned records. This partition is indicated Q (take note of that the cells don't necessarily should be the same size as the cells of P). Each cell in the partition Q must have the same number rmax of POI records. Any variation in this number could lead to the server identifying the client. In the event that this constraint cannot be satisfied, then sham records can be utilized to make beyond any doubt each cell has the same amount of data

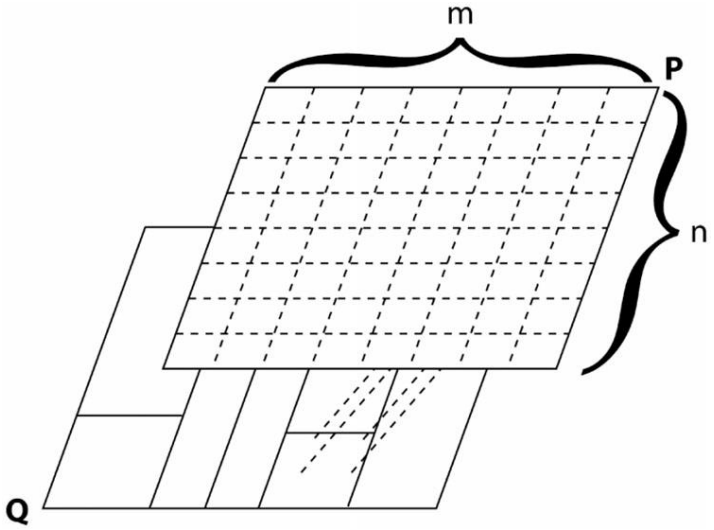


Fig. 3. Public grid superimposed over the private grid.

We assume that the LS does not populate the private lattice with misleading or incorrect data, since such action would bring about the loss of business under a payment model Next, the server scrambles each record ri within each phone of Q, Qi,j, with an associated symmetric key ki,j. The encryption keys are put away in a small (virtual) database table that associates each cell in general society framework P, Pi,j, with both a cell in the private lattice Qi,j and corresponding symmetric key ki,j. The server then procedures the encoded records within each cell Qi,j such that the client can utilize a productive PIR to inquiry the records. Using the private partition Q, the server speaks to each associated (encoded) data as an integer Ci, as for the cloaking locale. For each Ci, the server picks an arrangement of one of a kind prime forces $\pi i = pcii$ , such that $Ci < \pi i$. We take note of that the ci in the type must be small for the protocol to work proficiently.

**Private Information Retrieval Phase**

With the knowledge about which cells are contained in the Private grid and the knowledge of the key that encrypts the data in the cell, the user can initiate a private information Retrieval protocol with the location server to acquire the encrypted POI data. Assuming the server has initialized the integer e, the user ui and LS can engage in the following Private information retrieval protocol using the IDQi,j ,obtained from the execution of the previous protocol, as Input. The IDQi,j allows the user to choose the associated prime number power $\pi i$, which in turn allows the user to query the server.

At the conclusion of the protocol, the user has successfully acquired the block that contain the encrypted POI records. With the knowledge of the cell key ki,j, the user can decrypt Ci and obtain the requested data, thus concluding one round of the protocol. Using the same set-up, the user can execute several more rounds very efficiently and effectively without compromising his/her privacy. Similarly, the server's data remains protected based on the fact the user can only acquire one key per round. The security is analyzed in more detail next.

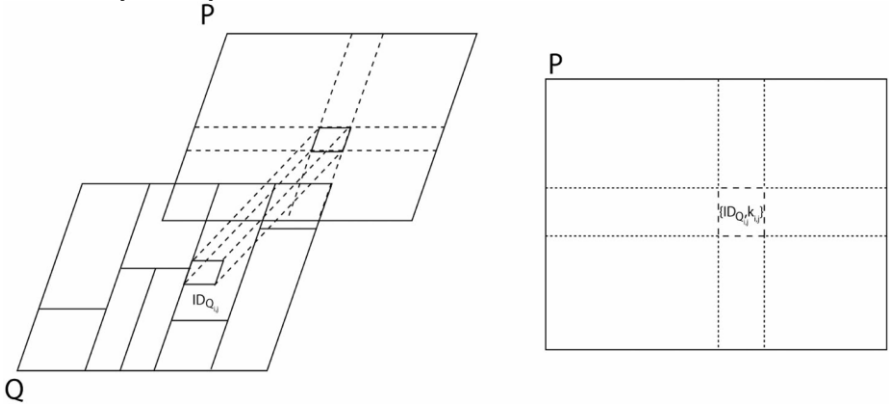


Fig. 4. Association between the public and private grids.

 

## VIII. SECURITY ANALYSES

In this section, we analyze the security of the client and The server. While the client does not want to give up the Privacy of his/her location, the server does not want to disclose other records to the client.

**Client's Security**

Fundamentally, the information that is most valuable to the client is his/her location. This location is mapped to a cell Pi,j. In both phases of our protocol, the absent transfer based protocol and the private information retrieval based protocol, the server must not have the capacity to distinguish two questions of the customer from each other. We will now depict both cases separately. In the private information retrieval phase, the security of the customer is based on the Gentry-Ramzan private information retrieval protocol, which is based on the phi-hiding (φ-hiding) assumption .On the basis of the above security analysis, we can finish up with the following theorem. \

**Server's Security**

Intuitively, the server's security requires that the customer can recover one record just in each question to the server, and the server must not uncover other records to the customer in the reaction. Our protocol achieves the server's security in the neglectful transfer phase, which is based on the Naor-Pinkas unmindful transfer protocol In the private information retrieval phase, regardless of the fact that the customer can recover more than one scrambled records, he/she can decode one and only record with the encryption key kij recovered in the main phase. Based on the above analysis, we obtain the following result. Theorem 4: Assume that the discrete logarithm is hard and the Naor-Pinkas protocol is a protected neglectful transfer protocol, our protocol has server security. The cell key of the structure gRi ||gCj where gRi ,gCj are the line and segment keys, individually. On the off chance that the client inquiries the database once, the client can get one cell key as it were. Nonetheless, if the client questions the database twice, the client can get four cell keys. In this paper, we defeat this security weakness by using the cell key of the structure ggRi1 gCj20, where both key parts are ensured by the discrete logarithm issue.

## IX. PERFORMANCE EVALUATION

Our proposed work has achieved both user and server side privacy using a two stage protocol oblivious transfer stage and private information retrieval [pir] and is implemented using java as source code and apache tomcat. Compared to previous works we have achieved a secure solution for both user and server using HMAC as well This is scalable and can be implemented in a smart phone. We analyzed the performance of our protocol and found it to be both computationally and communicationally more efficient.by using md5 we do not have limitation on the size of the file to be shared. Compared to previous work, we have achieved reasonable communication and CPU cost. It is better to use ATTP free protocol for location privacy in location-based services. While using these protocols we can fire only one query at a time. We have to enhance this protocol for executing number of queries at a time and can execute different types of spatial joins queries. In addition, we will enhance public grid in which group of users can determine his location at a time

## X. CONCLUSION

In this paper, we have displayed a location based question arrangement that utilizes two protocols that enables a client to privately determine and acquire their own particular location. Initially the client has to privately determine his/her location using negligent transfer on an open framework. The following stride involves a private information retrieval interaction that recovers the record with high communication productivity. Location privacy is a challenging research theme that involves both technological, legislative, and sociological issues past works have utilized Diffie Hellman strategy which is not productive, We have utilized md5 for encryption and decoding and SHA algorithm along with HMAC. To finish up, location information speaks to an important resource that can be utilized as a part of various situations and whose usage could offer colossal advantages to online services. Nonetheless, the conceivable in discriminated revelation of location information can summon a scenario in which location data are abused. In this way the productivity has been enhanced Secure arrangement, server and client side has been achieved. Using the above proposed protocol we have achieved a protected answer for both the parties.

## XI. FUTURE ENHANCEMENT

In future, we are going to execute our idea in mobile application, make it available for all mobile clients, as the idea is scalable many more clients can be included, and it can be actualized in smart phones. Consequently, the proposed protocol is within practical cutoff points and is communicationally more effective compared to past works.

## 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.

 