iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** III **Month of publication:** March 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Location Based Service without Reveling Self Privacy Data

D. Kanchana[1], Nandhini. C.S[2]
[1]Sri Venkateshwara College of Engineering and Technology, India
[2]Sri Venkateshwara College of Engineering and Technology, India

Abstract: - In this paper, I proposed to solve problems associated with the location data. The user does not want to send his location data (GPS coordinate) to the server directly, since doing so the server can find the user's location preferences and use that data for advertising the user's privacy is lost. The second part is like the server wants to protect its data from the user query. The server want to return back only relevant data to the user .The server cannot send back other sensitive data to the user. Location Based System (LBS) are used for finding out point of interests (POI) from a specific location. GPS latitude and longitude (GPS Coordinate) input to location servers, the POI can be served back to client from the location server. I propose a major enhancement upon previous solutions by introducing a two stage approach, to achieve a secure solution for both parties. Oblivious Transfer (OT), Private Information Retrieval (PIR), to achieve a secure solution for both parties. The solution we present is efficient and practical in many scenarios. I implement the solution using a real cloud location server and android mobile application.

Key Words:- Obvious Transfer, Point of Interest, Private Information Retrieval, location based query, Private query, Location monitoring, Location based service.

I. INTRODUCTION

A. Location Based Service (LBS)

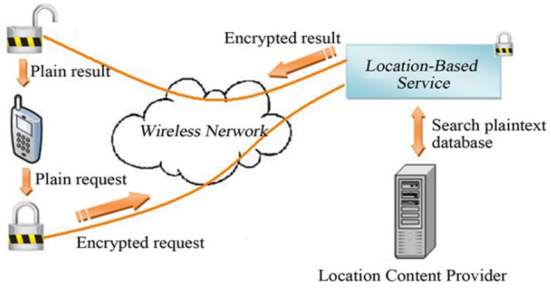
Location based service (LBS) is emerging as a killer application in mobile data services with the rapid development in wireless communication and location positioning technologies. Users with location-aware mobile devices can query their surroundings (e.g., finding all shopping centers within 5 miles or the nearest two gas stations from my current location) anywhere and at any time. However, although this ubiquitous computing paradigm brings great convenience for information access, the disclosure of user locations to service providers raises a concern of intrusion on location privacy, which has hampered the widespread use of LBS. Thus, how to enjoy LBS with preservation of location privacy has been gaining increasing research attention recently. In the literature, there are mainly two categories of approaches to preserve location privacy for LBS. The first is through information access control. User locations are sent to the service providers as usual. It relies on the service providers to restrict access to stored location data through rule-based polices. The second is to employ a trustworthy middleware running between the clients and the service providers. Each time a client makes a location based request, its location is anonymized by the middleware before being forwarded to the service providers. However, both of these two approaches are vulnerable to misbehavior of the third party. They offer little protection when the service provider middleware is owned by an untrusted party. There has been private data inadvertently disclosed over the Internet in the past. In this paper, we present iPDA, an alternative client based solution to enable privacy-preserving location-based data access for scenarios in which trust in third party is limited. In iPDA, a user can specify for each location-based query the privacy requirement with a minimum spatial area she wants to hide her location. For example, a user can specify it is acceptable to be located within an area of 1 square mile when she is in a shopping center or within an area of 10 square miles when she is in the Disneyland. Upon a location-based query (i.e., a range query or kNN query), iPDA cloaks user's current location with a region and transforms the location-based query to a region-based query.

Upon receiving the region-based query, the server evaluates and returns a result superset containing the query results for all location points in the cloak region. From the result superset, iPDA refines the actual result. There are number of challenging technical issues presented in iPDA, including 1) how to effectively cloak user locations to meet user-specified privacy requirements, and 2) how to efficiently evaluate result supersets for region based spatial queries. The idea of using cloaking to reduce location resolution is not new; it has been studied for years. However, all existing studies cloak user locations on a snapshot basis and have ignored the

spatial locality of client movement. Hence, the existing location cloaking algorithms can be attacked by mobility analysis. A user's location can be easily inferred if she makes queries frequently. We develop a mobility-aware cloaking technique to address this issue.

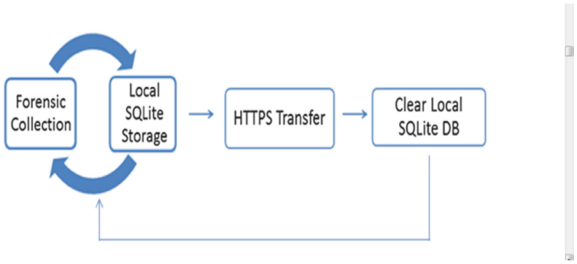
B. Android Application Development

Android is a software stack for mobile devices such as smart phones and tablet PCs. It was developed by the Open Handset Alliance, a consortium of 80 hardware, software, and telecommunication companies led by Google devoted to advancing open standards for mobile devices. Google purchased the initial developer of the software, Android Inc., in 2005. Android includes an operating system, middleware, and key applications. The Android SDK (Software Development Kit) provides the tools .Google released most of the Android code under the Apache License, a free software license. Android is tightly integrated with Google Maps, which provides a powerful tool for location-based services. Figure 3 shows a screenshot of a Google map with a location marker.



C. Location Monitoring

Droid Watch includes the device ID, latitude, longitude, and capture time. The approach that Droid Watch uses to collect locations conserves battery life, but results in the sparse logging of recorded locations. Only four locations over a seven-day period were reported. Even though the GPS provider setting was enabled, last known locations are not stored on a device unless the GPS is actively used (i.e., the Google Maps app is opened to display the current position). Furthermore, a phone's last known location value is cleared upon device reboots, causing a stored set of coordinates to be lost before being recorded. Changes made to the location provider setting are also available for tracking. This data would be potentially useful if the phone's physical location data becomes more reliable. It would allow for a device's location to be identified when its GPS setting is turned off manually.



D. Dentify Location With Privacy

In location based services (LBS), users with location aware 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 users' location privacy, which has hampered the widespread use of LBS. In this paper, we present new client based framework to facilitate privacy preserving location based data access in mobile environments.

The main idea is to reduce the resolution of user location based on location cloaking and transform a location based query to a region based query. We develop an optimal location cloaking technique that is immune to mobility analysis attack. We also propose efficient algorithms to process region base queries. Extensive experiments are conducted to demonstrate the effectiveness of the

propose algorithms.

E. Location Stored In Cloud

1) *Privacy Measure:* The k-anonymity is a commonly used model to specify privacy requirements in object tracking systems. In this model, an object location is cloaked with a region such that there exist at least k − 1 other objects in the same region. However, the k-anonymity model is not appropriate for location-based queries due to several reasons. First, it may incur excessive delay if less than k clients issue queries in a short period [9]. Second, it cannot work without knowing neighboring clients' locations in such a client-based framework as iPDA. As such, in this paper, we adopt a simple yet practical privacy measure, i.e., the spatial area of the cloak region. A user can specify a minimum acceptable cloak area with each query. Note that the cloak area requirement can achieve the same level of privacy protection as the k-anonymity model when the user density is available. In this case, we can set the area to be k.
2) *Region-Based Query Processing:* This section discusses circular-region-based query processing algorithms. The evaluation of a region-based range query is straightforward since it is still a range query (with extended range). Thus, we concentrate on the evaluation of circular-region-based kNN queries. Following Theorem 1, a circular-region-based kNN query can be decomposed into a range query and a kNN query of the circle's perimeter (denoted by). The kNN query of retrieves the set of kNNs for every point on (hereafter called k-*circular range- NN* —kCRNN query). In the following, we first propose kCRNN processing on an in-memory dataset, and then present three heuristics to prune unnecessary node accesses when applied to a spatial index of the dataset. Finally, we briefly discuss how to integrate the evaluation of a range query and a kCRNN query.

II. RELATED WORK

In this project I am using oblivious transfer and private information retrival.in early model uses non interactive oblivious transfer. This literature follows many related topics of those algorithm detailed in following below.

A. Oblivious Transfer

Bellare .M and Micali S, "Non-interactive oblivious transfer and applications,"

Oblivious transfer (OT) is a fundamental primitive used in many cryptographic protocols, including general secure function evaluation (SFE) protocols. However, interaction is a primary feature of any OT protocol. In this paper, we show how to remove the interaction requirement in an OT protocol when parties participating in the protocol have access to slightly modified Trusted Platform Modules, as defined by Sarmenta *et al.* in proposing the notion of count-limited objects (clobs). Specifically, we construct a new cryptographic primitive called "generalized non-interactive oblivious transfer"(GNIOT).

While it is possible to perform GNIOT using clobs in a straightforward manner, with multiple clobs, we show how to perform this efficiently, by using a single clob regardless of the number of values that need to be exchanged in an oblivious manner. Additionally, we provide clear definitions and a formal proof of the security of our construction. We apply this primitive to mobile agent applications and outline a new secure agent protocol called the GTX protocol which provides the same security guarantees as existing agent protocols while removing the need for interaction, thus improving efficiency.

B. Location Stored In Cloud

1) *Privacy Measure:* The k-anonymity is a commonly used model to specify privacy requirements in object tracking systems. In this model, an object location is cloaked with a region such that there exist at least k − 1 other objects in the same region. However, the k-anonymity model is not appropriate for location-based queries due to several reasons. First, it may incur excessive delay if less than k clients issue queries in a short period [9]. Second, it cannot work without knowing neighboring clients' locations in such a client-based framework as iPDA. As such, in this paper, we adopt a simple yet practical privacy measure, i.e., the spatial area of the cloak region. A user can specify a minimum acceptable cloak area with each query. Note that the cloak area requirement can achieve the same level of privacy protection as the k-anonymity model when the user density is available. In this case, we can set the area to be k.
2) *Region-Based Query Processing***:** This section discusses circular-region-based query processing algorithms. The evaluation of a region-based range query is straightforward since it is still a range query (with extended range). Thus, we concentrate on the evaluation of circular-region-based kNN queries. Following Theorem 1, a circular-region-based kNN query can be decomposed

into a range query and a kNN query of the circle's perimeter (denoted by). The kNN query of retrieves the set of kNNs for every point on (hereafter called k-*circular range- NN* —kCRNN query). In the following, we first propose kCRNN processing on an in-memory dataset, and then present three heuristics to prune unnecessary node accesses when applied to a spatial index of the dataset. Finally, we briefly discuss how to integrate the evaluation of a range query and a kCRNN query.

III. SYSTEM ANALYSIS

System Analyais is the process of analyzing the system and its component. It deals with what did the existing system and what I am going do in proposed system are detailed below.

A. Existing System

Preserving data privacy has been extensively studied for general database applications. However, relatively fewer works have studied protection of location privacy for location based services. Most of the existing studies focused on object location tracking. A typical solution is to employ a trustworthy third-party middleware to collect exact locations from moving clients and anonymize location data through de-personalization before release. Beresford and Stajano define some geographical regions as *mix zones*. Once a client enters into a mix zone, its identity is mixed with all other users in the zone.

Gruteser and Grunwald provide location anonymity by spatio-temporal cloaking based on the k-anonymity model. A Quad-tree like algorithm is used to perform spatial cloaking. Gedik and Liu extended it to a personalized k-anonymity model. Users can also specify the minimum acceptable spatial resolution and temporal tolerance. A new cloaking algorithm called Clique Cloak was developed. However, these previous studies did not consider the spatial locality of client movement in location cloaking. Moreover, the query processing issue has been left out in these studies.

The existing system uses two stage approaches to preserve privacy for users and location service provider and implements better solution for privacy over two communications like users to service provider and service provider to location server.

1) *Disadvantage:* LS (Location Server) supplying misleading data to the client, This misleads about integration of all the model.

B. Proposed System

The proposed system uses a real cloud implementation of the location server. The data which server has is completed protected from the user. As well the location information (GPS coordinate) of the user is never sent directly instead only a grid information will be sent. We will be implementing the client using an android mobile.

1) *Advantages***:** We overcome the data misleading between location server and users.We provide better security algorithm to protect user's information during transformation. Realtime using cloud and android mobile.

C. System description

System description deals with the modules what we are developing the modules for developing the project. It specifies the details of the system.

D. Modules Description

Modules means emphasizes separating the functionality of a program into a independent interchangeable, such that each contains everything necessary to execute only one aspect of the desired functionality. This is the stage of the project when the theoretical design is turned out in to a working system.

1) *Module 1: Get Location:*
   a) *Client:* Android Mobile application will send the user grid information to the server and security key will decrypt the data. We will be using the symmetric encryption key.
   b) *Server:* The server will super impose the user cell information with the server location grid and find the location server's grid cell information. The server's cell information will be sent back to the user.
2) *Module 2: User query:*
   a) *Client:* The client will send the request using the server's cell information asking for the point of interest say a shopping mall nearby.

b) Server: The server will return the encrypted data of the point of interest to the client will plot the information in the graph.

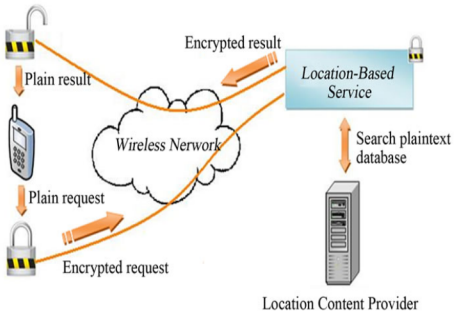
3) *Module 3: Privacy Identification:*

a) Client: The request sent by the client will use the symmetric encryption key to encrypt all the data. Further the connection between server and client will be secure.

b) Server: The server will also send all the information encrypted using the key sent by the client. The communication between client and server will be secure. The client will never send the GPS coordinate but will send an information grid of its location.

E. System Architecture Diagram

A system architecture or systems architecture is the conceptual design that defines the structure and/or behavior of a system. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks...and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system.



F. Security Model

Our initialisation phase is run by the sender (server),who owns a database of location data records and a 2-dimensional key matrix K$m\times n$, where m and n are rows and columns respectfully. An element in the key matrix is referenced as ki,j. Each ki,j in the key matrix uniquely encrypts one record. A set of prime powers S = {$pc1$, . . . , pcN }, where 1 N N is the number of blocks, is available to the public. Each element in S the pi is a prime and ci is a small natural number such that pci is greater than the block size (where each block contains a number of POI records). We require, for convenience that the elements of S follow a predictable pattern. In addition, the server sets up a common security parameter k for the system.

Our transfer phase is constructed using six algorithms:

QG1,RG1,RR1,QG2,RG2,RR2. The first three compose the first phase (Oblivious Transfer Phase), while the last threecompose the second phase (Private Information Retrieval Phase). The following six algorithms are executed sequentially and are formally described as follows.

G. Oblivious Transfer Phase

1) *QueryGeneration*1 (*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) *ResponseGeneration*1(*Server*) (RG1):

Takes as input the key matrix K$m\times n$, and the query Q1, and outputs a response R1, denoted as (R1) = $RG1$(K$m\times n$, Q1).

3) *ResponseRetrieval*1 (*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 cellkey ki,j and cell-id IDi,j, denoted as (ki,j, IDi,j) = $RR1(i, j, m, n,$ ($Q1$, $s1$), R1).

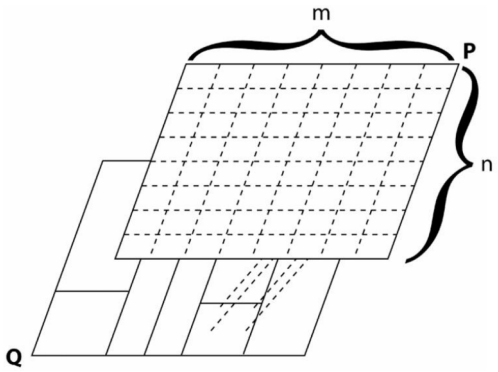
H. Private Information Retrieval Phase

4) *QueryGeneration*2 (*Client*) (QG2): Takes as input the cell-id IDi,j, and the set of primepowers S, and outputs a query Q2 and secret $s2$,denoted as (Q2, $s2$) = $QG2(IDi,j,$ S).

5) *ResponseGeneration*2 (*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) = *RG*2(*D*, Q2, S).
6) *ResponseRetrieval*2 (*Client*) (RR2): Takes as input the cell-key *ki,j* and cell-id *IDi,j*, the query Q2 and secret *s*2, the response R2, and outputs the data *d*, denoted as (*d*) = *RR*2(*ki,j*, *IDi,j*, (Q2, *s*2), 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.

I. Protocol Summary

The ultimate goal of our protocol is to obtain a set (block) of POI records from the LS, which are close to the user'sposition, without compromising the privacy of the user or the data stored at the server. We achieve this by applying a two stage approach shown in Fig. 2. The first stage is based on a two-dimensional oblivious transfer [26] and the second stage is based on a communicationally efficient PIR [11]. The oblivious transfer based protocol is used by the user to obtain the cell ID, where the user is located, and the corresponding symmetric key. The knowledge of the cell ID and the symmetric key is then used in the PIR based protocol to obtain and decrypt the location data. The user determines his/her location within a publicly generated grid *P* by using his/her GPS coordinates and forms an oblivious transfer query2. The minimum dimensions of the public grid are defined by the server and are made available to all users of the system. This public grid superimposes over the privately partitioned grid 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 the public grid. This is illustrated in Fig



Super imposed of public and private grid

IV. PERFORMANCE ANALYSIS

We now analyse the performance of our solution and show that it is very practical. The performance analysis consists of the computation analysis and the communication analysis. We supplement this analysis with a comparison with the protocol.

A. Computation

Since the most expensive operation in our protocol is the modular exponentiation, we focus on minimising the number of times it is required. We assume that some components can be precomputed, and hence we only consider the computations needed at runtime. Furthermore, we reduce the number of exponentiations required by the PIR protocol to the number of multiplications that are required. This will make the computational comparison between our solution and the solution of Ghinita *et al.* easier to describe.The transfer protocol is initiated by the user, who chooses indices *i* and *j*. According to our protocol the user needs to compute (*A*1, *B*1) = (*gr*1 *i r*1) and (*A*2, oth *y*1 and *y*2 (i.e. *x*1 and *x*2 respectively), the user can compute (*A*1, *B*1) and (*A*2, *B*2) as (*A*1, *B*1) = (*gr*1 , *g*−*i*+*x*1 *r*1) and PIR protocol. The size of number *e* is principally defined −*j x*2 *r*2 1 1 by*N* the prime powers. *gr*2 , *g* +) respectively. *i*=1 *log*2(*πi*) bits to store *e* and we would expect to be compute 4 exponentiations to generate his/her query. multiplying η/2 of the time using the square-and-multiply.

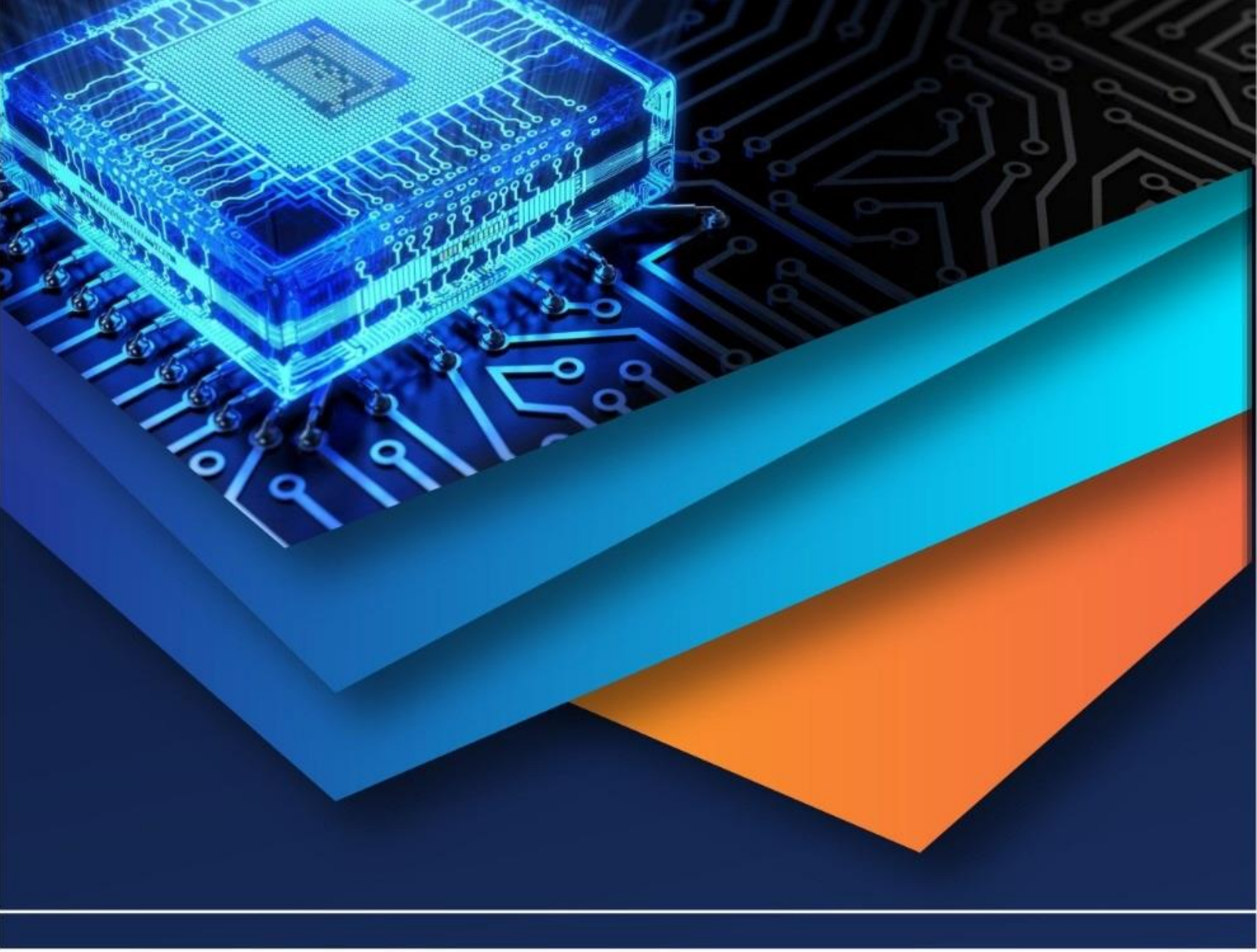
V. CONCLUSION

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 Ghinita *et 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 manydifferent 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] Agrawal .D *PODS*, 2001 and Aggarwal. C. On the design and quantification of privacy preserving data mining algorithms.
[2] Berchtold .S, Bohm. C, Keim D.A, Krebs .F, and Kriegel H.-P. .*ICDT* 2001On optimizing nearest neighbor queries in highdimensional data spaces.
[3] *IEEE Pervasive Computing*, Beresford A.R and Stajano. F.V. 2003 Location privacy in pervasive computing.
[4] Cheng .R, Kalashnikov D, and Prabhakar P, *TKDE*, 2004. Querying imprecise data in moving object environments.
[5] Emekc. F, Agrawal D, Abbadi A. E, nd Gulbeden A. *ICDE*, 2006 Privacy preserving query processing using third parties.
[6] [Online] http://www.ietf.org/ html.charters/geopriv-charter.html, 2005. Geopriv Working Group.
[7] Friday A , and Davies N. *IEEE Pervasive Computing*, 2(1):56–64, 2003 Myles Preserving privacy in environments with location-based applications.
[8] Gruteser M and Grunwald D. 2008Anonymous usage of location-based services through spatial and temporal cloaking.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY