PRIVACY-PRESERVING AND CONTENT-ROTECTING LOCATION BASED QUERIES

[1]Muthe Hemant, [2]Shingote Navin, [3]Mrs. More Priyanka

Abstract— In this paper we have a tendency to gift an answer to 1 of the location-based question issues. This downside is outlined as follows: (i) a user needs to question a information of location information, called Points Of Interest (POIs) and doesn't need to reveal his/her location to the server because of privacy concerns; (ii) the owner of the placement information, that is, the placement server, doesn't need to easily distribute its data to all or any users. the placement server wishes to possess some management over its information, since the information is its plus. we have a tendency to propose a serious enhancement upon previous solutions by introducing a 2 stage approach, wherever the primary step is predicated on Oblivious Transfer and the second step is predicated on non-public data Retrieval, to realize a secure resolution for each parties. the answer we have a tendency to gift is efficient and sensible in several eventualities. we have a tendency to implement our resolution on a desktop machine and a mobile device to assess the efficiency of our protocol. we have a tendency to conjointly introduce a security model and analyse the safety within the context of such protocol. Lastly, we specify a security drawback of the previous work we did and gift an answer to beat it.

Index Terms—Queries based on location, private queries, retrieval of private information, oblivious transfer.

I INTRODUCTION

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 users supported the geographical position of their mobile device. The services provided by a LBS ar usually supported a degree of interest database. By retrieving the Points Of Interest (POIs) from the information server, the user will get answers to varied location based mostly queries, that embody however don't seem to be restricted to - discovering the closest ATM machine, petrol station, hospital, or station. In recent years 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, users might feel reluctant to disclose their locations to the LBS, as a result of it should be doable for a location server to learn United Nations agency is creating a definite question by linking these locations with a residential phone book information, since users are doubtless to perform several queries from home. The Location Server (LS), that offers some LBS, spends its resources to compile data regarding varied fascinating POIs. Hence, it's expected that the LS wouldn't disclose any data while not fees. So the LBS has to make sure that LS's knowledge isn't accessed by any unauthorized user. Throughout

the method of transmission the users should not be allowed to find any data for which they need not paid. it's so crucial that solutions be devised that address the privacy of the users issue queries, however additionally forestall users from accessing content to which they are doing not have authorization. The ultimate goal of our protocol is to get a collection (block) of dish records from the LS, that ar near the user's position, while not compromising the privacy of the user or the data keep at the server the foremost high-priced operation in our protocol is that the modular operation, we have a tendency to target minimising the quantity of times it's needed. we have a tendency to assume that some parts can be precomputed, and thence we have a tendency to solely take into account the computations required at runtime we have a tendency to analysed the performance of our protocol and located it to be each computationally and communicationally additional efficient than the answer by Ghinita et al., that is that the most recent resolution. we have a tendency to enforced a code model using a desktop machine and a mobile device. The code prototype demonstrates that our protocol is at intervals sensible limits.

the location server, doesn't need to easily distribute its information to any or all users. the placement server wishes to own some management over its information, since the info is its plus. Previous solutions have used a sure anonymiser to deal with privacy, however introduced the inutility of trusting a 3rd party. more moderen solutions have used homomorphic cryptography to get rid of such weakness. Mainly, the user submits ones coordinates those are encrypted to the server and therefore the server would verify the user's location homomorphically, so the user would acquire the corresponding record victimization personal info Retrieval techniques. we have a tendency to propose a significant improvement upon this result by introducing an identical 2 stage approach, wherever the homomorphic comparison step is replaced with Oblivious Transfer to attain a safer resolution for each parties. the answer we have a tendency to gift is economical and sensible in several eventualities. we have a tendency to conjointly embody the results of a operating epitome for instance the potency of our protocol.

• II Literature Survey

M. Bellare and S. Micali [2]. They are proposed an client and fair proto col for secure two-party computation in the Optimistic model, in which a partially trusted 3rd party T is available, but not in volved in normal executions of protocol. T is required only if there exist disruption in communication or if one Of the two parties denies or misbehaves. This protocol ensures that even if 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 client proofs of knowledge and involve no general zero-knowledge to ols as intermediate steps we describe e±cien tveriØ-able oblivious transfer.

A. Beresford and F. Stajano[3] they are proposed an As location-aware applications begin to track our movements in the name of convenience, how can we protect our rivacy? This article introduces the mix zone-a new construction inspired by anonymous communication techniques-together with metrics for assessing anonymity of an user which is based on pseudonyms which are frequently changing.

C. Bettini, X. Wang, and S. Jajodia[4] They proposed an manuscript & we present a solution to one of the location predicated query quandaries. This quandary is defined as follows: (i) a utilizer wants to query a database of location data, kenned as Points Of Interest (POIs) and does not optate 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 optate to simply distribute its data to all the users. Here the location server wishes to have some control over its data, since the data is its asset. We recommend a major enhancement upon anterior solutions by introducing a two stage approach, where the first step is predicated on Oblivious Transfer and the second step is predicated on Private Information Retrieval (PIR), so as to achieve a secured solution for both the parties. The solution which we present is quite efficient and more practical in many of the scenarios. We then implement our solution onto a desktop machine and a mobile contrivance to assess the efficiency of our protocol. We additionally introduce a security model and analyze the security in the context of our

protocol. Finally, we highlight a security impotency of our an tecedent work and present a solution to surmount it.

X. Chen and J. Pang[5] They proposed an Vehicular networks are envisioned to play an important role in the building of intelligent transportation systems. However, the dangers of the wireless transmission of potentially exploitable information such as detailed locations are often overlooked or only inadequately addressed in field operational tests or efforts of standardization. The main reasons for this is that the concept of privacy is difficult 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 protection mechanism. In this paper we discuss the principles, all the challenges, and also the necessary steps in terms of privacy assessment in vehicular N/Ws. We also identify all useful and the practical metrics that allow the comparison and evaluation of privacy protection algo's. We hereby present a very systematic literature review that sheds light on the current state of the art and give recommendations for future research directions in the field.

B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan[6] the proposed a survey the notion of Single-Database Private Information Retrieval (PIR). The first Single-Database PIR was constructed in 1997 by Kushile vitz and Ostrovsky and since then Single-Database PIR has emerged as an important primitives of cryptography. For ex., Single-Dbase PIR turned out to be intimately connected to collision-resistant hash functions, the oblivious transfer and also public-key encryptions with some additional properties. Here in this survey, we state an overview of many of the constructions for Single-Database PIR (including an abstract construction based upon homomorphic encryption) and describe some of the connections of PIR to other primitives.

T. ElGamal[9] proposed A new signature scheme, together with the implementation of the Diffie-Hellman public key distribution scheme that achieves a public key cryptosystems. The secureness of the both systems relies on the difficulty of computing discrete logarithms over finite fields.

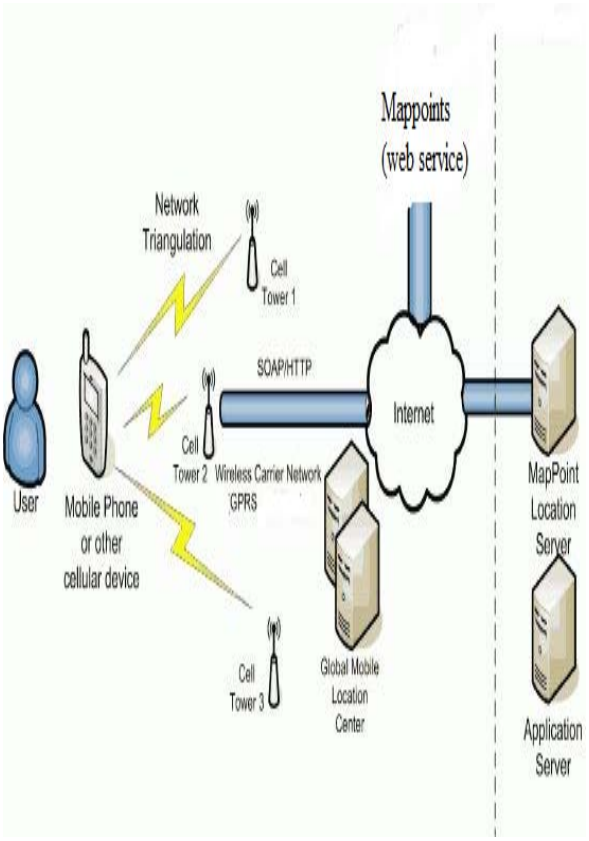
B. Gedik and L. Liu[10] they are proposed a solution to one of the location predicated query quandaries. This quandary is defined as follows: (i) a utilizer wants to query a database of location data, kenned as Points Of Interest (POIs) and does not optate to reveal his/her location to the server due to privacy concerns; (ii) the owner of the location data, that is, the location server, does not optate to simply distribute its data to all the users. Here the location server wishes to have some control over its data, since the data is its asset. We recommend a major enhancement upon anterior solutions by introducing a two stage approach, where the first step is predicated on Oblivious Transfer and the second step is predicated on Private Information Retrieval, so as to achieve a very secure solution for both the parties. The solution which we present is too efficient and practical in most of the scenarios. We then implement our solution to/on a desktop machine and a mobile contrivance to assess the efficiency of our protocol. We additionally introduce a security model and analyze the security in the context of our protocol. Finally, we highlight a security impotency of our an tecedent work and present a solution to surmount it.

C. Gentry and Z. Ramzan[11] the are proposed an location with the help of devices having GPS facility. When user's location is provided to LBS, it is possible to user to know all location dependent information like location of friends or Nearest Restaurant, whether or traffic conditions. The massive use of mobile devices pave the way for the creation of wireless networks that can be used to exchange information based on locations of users. When we get done with exchange of location information amongst entrusted parties, the privacy of the user could be in harmful. Existing protocol doesn't work on many different mobile devices and another issue is that, Location Server (LS) should provide misleading data to user. So we are working on enhancement of this protocol. Mobile devices with global positioning capabilities allow users to retrieve points of interest (POI) in their proximity area. To protect the user privacy, its important not to disclose exact user coordinates to un-trusted entities that provide location-based
services. Currently, there are two main approaches to protect the location privacy of users: (i) hiding locations inside cloaking regions

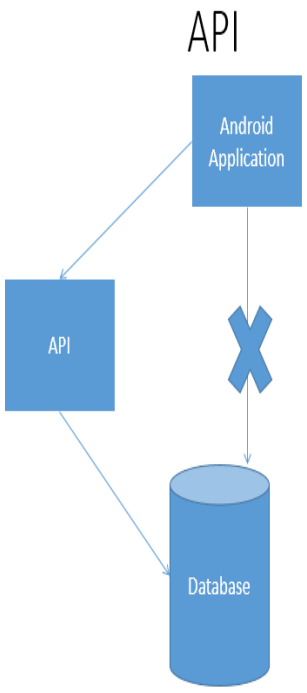
(CRs) and (ii) encrypting location data using private information retrieval (PIR) protocols. Our previous work mainly focused on discovering good trade-offs between privacy and user protection techniques performances, but it disregarded the most important issues of protecting the POI dataset D. For the instance, location cloaking requires large-sized CRs, leading to excessive disclosureof POIs (O(D)in its worst case). PIR (private information retrival), on the other hand, minimizes this bound to O(√D|), but at the expense of high processing and the communication overhead. We therefore proposed a hybrid, two-step approache for private location-based queries which provide protection for both the users and also the database. In the very first step, user locations are hence generalized to coarse-grained CRs which provide strongest privacy. Next: a PIR protocol is applied with respect to the obtained query CR. To protect against excessive disclosure of POI(point of interest) locations, we devise two cryptography protocols which privately evaluate whether a point is enclosed inside a rectangular region or a convex polygon. We also state algorithms to efficiently support PIR on dynamic POI.

III Proposed System

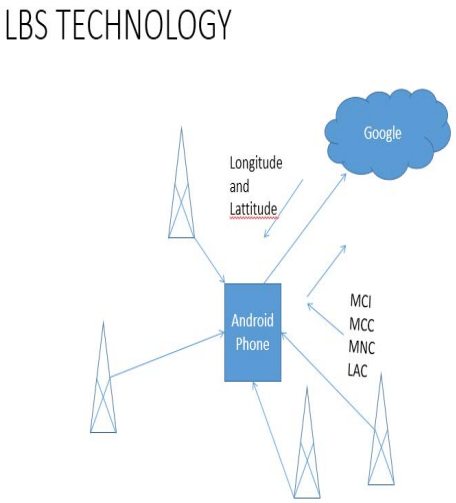
In this system we involve testing the protocol on several different mobile devices. The mobile result we offer may be completely different than alternative mobile devices and computer code environments. Also, we'd like to cut back the overhead of the property take a look at utilized in the personal info retrieval based protocol. in addition, the matter regarding the L.S supply deceptive information to the consumer is additionally attention-grabbing. Privacy protective name techniques appear a suitable approach to deal with such drawback. A possible solution may integrate strategies. Once appropriate strong solutions exist for the overall case, they'll be simply integrated into our approach.



Architecture Diagram.1



Architecture Diagram 2



LBS Technology

This algorithm uses the location indexes of the users and multiple parallel threads to search and select quickly all the candidate anonymous sets with more users and their location information with more uniform distribution to accelerate the execution of the temporal-spatial anonymous operations, and it allows the users to configure their custom-made privacy-preserving location query requests.

- **IV Work Done**

4.1 Input screen

Login screen: The below figure shows the login screen of location sharing.

Figure1. Login screen

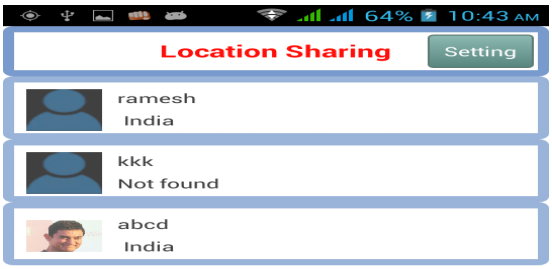


Figure 2- Output Screen

4.2 Hardware and Software Used

Hardware Configuration

- Processor - Pentium –IV
- Speed - 1.1 GHz
- RAM - 256 MB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Monitor - SVGA

Software Configuration

- Operating System: Windows XP/7/8
- Programming Language: java
- DATABASE: MySQL
- Tool: Net bins

V Mathematical Module

Algorithm 1: Initialization

Input:

Output :

1**:** ,for 1

Where

2:

Where H is a fats secure hash function

3: return

Algorithm 2 $Transfer$

Input: **User:**i, j
Output: **User:**$(ID_{Q_{i,j}}, k_{i,j})$

1: **User** $(QG1)$
2: $y_1 \leftarrow g_1^{x_1}$, where y_1 is the public key for the row and x_1 is chosen at random
3: $y_2 \leftarrow g_2^{x_2}$, where y_2 is the public key for the column and x_2 is chosen at random
4: $\boldsymbol{C_1} \leftarrow (A_1, B_1) = (g_1^{r_1}, g_1^{-i} y_1^{r_1})$
5: $\boldsymbol{C_2} \leftarrow (A_2, B_2) = (g_2^{r_2}, g_2^{-j} y_2^{r_2})$
6: $Server \Leftarrow \boldsymbol{C_1}, \boldsymbol{C_2}$
7: **Server** $(RG1)$
8: $\boldsymbol{C'_{1,\alpha}} \leftarrow (A_1^{r'_\alpha}, g_1^{R_\alpha} r_R (g_1^\alpha B_1)^{r'_\alpha})$ for $1 \leq \alpha \leq n$ and $r_R = g_1^s$, where s is chosen randomly
9: $\boldsymbol{C'_{2,\beta}} \leftarrow (A_2^{r'_\beta}, g_2^{C_\beta} r_C (g_2^\beta B_2)^{r'_\beta})$ for $1 \leq \beta \leq m$ and $r_C = g_2^t$, where t is chosen randomly
10: $\gamma \leftarrow g_0^{1/r_R r_C}$
11: $User \Leftarrow \boldsymbol{C'_{1,1}}, ..., \boldsymbol{C'_{1,n}}, \boldsymbol{C'_{2,1}}, ..., \boldsymbol{C'_{2,m}}, \gamma$
12: **User** $(RR1)$
13: Let $(U_{1,i}, V_{1,i}) = \boldsymbol{C'_{1,i}}$ and $(U_{2,j}, V_{2,j}) = \boldsymbol{C'_{1,j}}$
14: $W_1 \leftarrow U_{1,i}^{-x_1}$
15: $W_2 \leftarrow U_{2,j}^{-x_2}$
16: $W_3 \leftarrow V_{1,i} W_1$
17: $W_4 \leftarrow V_{2,j} W_2$
18: $K'_{i,j} \leftarrow \gamma^{W_3 W_4}$
19: $X'_{i,j} \leftarrow Y_{i,j} \oplus H(K'_{i,j})$
20: Reconstruct $(ID_{Q_{i,j}}, k_{i,j})$ from $X'_{i,j}$
21: **return** $(ID_{Q_{i,j}}, k_{i,j})$ {Cell id of grid Q, with associated cell key}

• VI Conclusion and Future Work

In this paper we've got given a location based mostly question solution that employs 2 protocols that permits a user to in private verify and acquire location information. The first step is for a user to in private verify his/her location using oblivious transfer on a public grid. The second step involves a non-public info retrieval interaction that retrieves the record with high communication potency. We analysed the performance of our protocol and located it to be each computationally and communicationally a lot of efficient than the answer by Ghinita et al., that is that the most recent resolution. we tend to enforced a software system epitome using a desktop machine and a mobile device. The software system prototype demonstrates that our protocol is among sensible limits.

• VII 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 the Proc._CRYPTO, 1990, pp.(547–557).

[3] A. Beresford and F.Stajano, " Location Privacy in Pervasive Computing ", IEEE Pervasive Compute., vol. 2, no.1, pp. (46–55), Jan.–March. 2003.

[4] C. Bettini, X. Wang, and S.Jajodia, "Protecting the 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.

[16] M. Gruteser and D. Grunwald, "Anonymous usage of locationbased services through spatial and temporal cloaking," in Proc. 1st Int. Conf. MobiSys, 2003, pp. 31–42.

[17] T. Hashem and L. Kulik, "Safeguarding location privacy in wireless ad-hoc networks," in Proc. 9th Int. Conf. biComp, Innsbruck, Austria, 2007, pp. 372–390.

[18] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," in Proc. 1st Int. Conf. SecureComm, 2005, pp. 194–205.

[19] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," IEEE Trans. Knowl. Data Eng., vol. 19, no. 12, pp. 1719–1733, Dec. 2007.

[20] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in Proc. Int. Conf. ICPS, 2005, pp. 88–97.

[21] J. Krumm, "A survey of computational location privacy," Pers. Ubiquitous Comput., vol. 13, no. 6, pp. 391–399, Aug. 2009.

[22] E. Kushilevitz and R. Ostrovsky, "Replication is not needed: Single database, computationally-private information retrieval,"in Proc. FOCS, Miami Beach, FL, USA, 1997, pp. 364–373.

[23] L. Marconi, R. Pietro, B. Crispo, and M. Conti, "Time warp: How time affects privacy in LBSs," in Proc. ICICS, Barcelona, Spain, 2010, pp. 325–339.

[24] S. Mascetti and C. Bettini, "A comparison of spatial generalization algorithms for lbs privacy preservation," in Proc. Int. Mobile Data Manage., Mannheim, Germany, 2007, pp. 258–262.

[25] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," in Proc. VLDB, Seoul, Korea, 2006, pp. 763–774.