© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Protecting Privacy against Location-Based Personal Identification

Ram Prakash. R, Prabhu. K, Samson Sunny. S, Devi. S
Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India

ABSTRACT

In this paper we exhibit an answer for one of the area based inquiry issues. This issue is characterized as tails: (i) a client needs to inquiry 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 protection concerns; (ii) the holder of the area information, that is, the area server, would not like to just appropriate its information to all clients. The area server goals to have some control over its information, subsequent to the information are its advantage. We propose a noteworthy upgrade upon past arrangements by presenting a two stage approach, where the first step is in view of Oblivious Transfer and the second step is taking into account Private Information Retrieval, to attain to a protected answer for both sides. The arrangement we present is proficient and viable in numerous situations. We actualize our answer on a desktop machine and a cell phone to evaluate the proficiency of our convention. We additionally present a security demonstrates and dissects the security in the setting of our convention. At last, we highlight a security shortcoming of our past work and present an answer for overcome it.

Keywords: Location based query, private query, private information retrieval, oblivious transfer

I. INTRODUCTION

A Location based administration (LBS) is a data, stimulation 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 commonly in light of a state of investment database. By recovering the Points of Interest (POIs) from the database server, the client can get answers to different area based inquiries, which incorporate yet are not restricted to - finding the closest ATM machine, service station, healing facility, On the other hand police headquarters. Lately there has been an emotional increment in the quantity of cell phones questioning area servers for data about POIs. Among numerous testing hindrances to the wide organization of such application, security confirmation is a noteworthy issue. For example, clients may feel hesitant to reveal their areas to the LBS, in light of the fact that it might be workable for an area server to realize who is making a certain question by connecting 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 incorporate data about different intriguing POIs. Thus, it is normal that the

LS would not uncover any data without expenses. In this manner 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 subsequently vital that arrangements be formulated that address the protection of the clients issuing questions, additionally keep clients from getting to substance to which they don't have approval.

II. METHODS AND MATERIAL

A. Related Work

The principal answer for the issue was proposed by Beresford [4], in which the security of the client is kept up by always showing signs of change the client's name or nom de plume inside some blend zone. It can be demonstrated that, because of the nature of the information being traded between the client and the

server, the continuous changing of the client's name gives little insurance for the client's protection. A later examination of the blend zone methodology has been connected to street systems [30]. They examined the obliged number of clients to fulfill the unsinkability property when there are rehashed inquiries over an interim. This obliges watchful control of what number of clients is contained inside the blend zone, which is hard to attain to practically speaking.

A corresponding strategy to the blend zone approach is in light of k-secrecy [5], [11], [17]. The idea of k-namelessness was presented as a system for saving protection when discharging touchy records [33]. This is attained to 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 anon miser to give obscurity to the area information, such that the area information of a client can't be recognized from (k − 1) different clients. An updated trusted anonymiser strategy has moreover been proposed, which allows the customers to set their level of security in perspective of the estimation of k [25], [26]. This implies that, given the overhead of the anonymiser, a little estimation of k could be utilized to build the proficiency. Then again, a vast 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 vindictively. Picking a quality for k, on the other hand, appears to be unnatural. There have been endeavors to make the process less simulated by including the idea of feeling-based security [24], [34]. Instead of showing a k, they suggest that the customer demonstrates a covering territory that they feel will guarantee their security, and the structure sets the amount of cells for the district in perspective of the pervasiveness of the zone. The frame is figured by utilizing verifiable foot shaped impression database that the server gathered. New security measurements have been recommended that catches the clients' security regarding LBSs [6]. The creators start by investigating the deficiencies of basic k-namelessness in the setting of area questions. Next, they propose security measurements that empower the clients to indicate values that better match their question security prerequisites. From these security measurements they likewise propose spatial speculation calculations that harmonize with the client's security necessities. Routines have likewise been proposed to befuddle and bend the area information, which incorporate way and position disarray. Way disarray was displayed by Hoh and Gruteser [19]. The essential thought is to add vulnerability to the area information of the clients at the focuses the ways of the clients cross, making it difficult to follow clients in view of crude area information that was k-anonymised. Position disarray has likewise been proposed as a way to give protection [20], [26]. The thought is for the trusted anonymiser to gathering the clients agreeing to a shrouding area (CR), therefore making it harder for the LS to recognize a single person. A typical issue with general CR strategies is that there may exist some semantic data about the geology of an area that doles out the client's area. For instance, it would not bode well for a client to be on the water without a watercraft. Likewise, distinctive individuals may discover certain spots touchy. Damiani et al. have exhibited a structure that comprises of an obscurity motor that takes a client's profile, which contains places that the client esteems touchy, and yields muddled areas taking into account collecting calculations [8]. As arrangements in light of the utilization of a focal anonymiser are not useful, Hashem and Kulik displayed a plan whereby a gathering of trusted clients build a specially appointed system also, the undertaking of questioning the LS is designated to a solitary client [18]. This thought enhances the past work by the truth that there is no single purpose of disappointment. On the off chance that a client that is questioning the LS abruptly goes disconnected from the net, then an alternate competitor can be effortlessly found. Notwithstanding, producing a trusted adhoc system in a true situation is not generally conceivable. An alternate technique for keeping away from the utilization of a trusted anonymiser is to utilize "sham" areas [9], [21]. The fundamental thought is to befuddle the area of the client by sending numerous irregular different areas to the server, such that the server can't recognize the genuine area from the fake areas. This causes both handling and correspondence overhead for the client gadget. The client needs to arbitrarily pick an arrangement of fake areas and additionally transmitting them more than a system, squandering data transfer capacity. We allude the intrigued peruser to Krumm [22], for a more nitty gritty study here. The greater part of the beforehand talked about issues are illuminated with the presentation of a private data recovery (PIR) area plan [15]. The essential thought is to utilize PIR to empower the client to inquiry the area database without bargaining the

protection of the question. As a rule, PIR plans permit a client to recover information (bit or piece) from a database, without uncovering the file of the information to be recovered to the database server [7]. Ghinita et al. utilized a variation of PIR which is in light of the quadratic residuosity issue [23]. Basically the quadratic residuosity issue expresses that is computationally hard to make sense of if a number is a quadratic store of some composite modulus n (x2 = q (mod n)), where the factorisation of n is dark. This musing was contacted give database security [13], [14]. In the first stage, the client and server use homomorphic encryption to permit the client to secretly figure out if his/her area is contained inside a cell, without uncovering his/her directions to the server. In the second stage, PIR is utilized to recover the information contained inside the proper cell. The homomorphic encryption plan used to secretly analyze two whole numbers is the Paillier encryption plan [28]. The Paillier encryption plan is known to be additively homomorphic and multiplicatively-by-a-consistent homomorphic. This implies that we can include or scale numbers actually when all numbers are scrambled. Both peculiarities are used to focus the sign (most huge bit) of (a − b), what's more, subsequently the client has the capacity focus the cell in which he/she is found, without unveiling his/her location.

B. Our Contributors

In this paper, we propose a novel convention for area based questions that has real execution changes as for the methodology by Ghinita at el. [13] and [14] .Like such convention, our convention is sorted out as indicated by two stages. In the first stage, the client secretly decides his/her area inside an open lattice, utilizing negligent exchange. This information contains both the ID and related symmetric key for the square of information in the private framework. In the second stage, the client executes a communicational proficient PIR [12], to recover the suitable piece in the private lattice. This square is unscrambled utilizing the symmetric key acquired in the past stage. Our convention along these lines gives security to both the client what's more, the server. The client is secured in light of the fact that the server is not able to focus his/her area. Additionally, the server's information is ensured since a malevolent client can just decode the square of information got by PIR with the encryption key procured in the past stage. As it were, clients can't increase any more information than what they have paid for. We comment that this paper is an improvement of a past work [29]. Specifically, the accompanying commitments are made.

1) Redesigned the key structure
2) Added a formal security model
3) implemented the arrangement on both a cell phone also, desktop machine similarly as with our past work, the execution shows the productivity and reasonableness of our approach.

C. Paper Organization

Whatever remains of the paper is composed as takes after. Area 2 presents the convention model and different preliminaries. Segment 3 presents and portrays our proposed convention. Segment 4 examinations the security of the convention. Segment 5 examinations the execution and effectiveness of the convention. Segment 6 reports the execution aftereffects of a working model utilizing two stages: a desktop and a portable, also, talks about plausibility. Area 7 compresses the key commitments of this paper and future headings.

D. Protocol Model

i. System Model

The framework model comprises of three sorts of substances: 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 have to be concerned with the specifics of the correspondence. The clients in our model utilize some area based administration given by the area server LS. For instance, what is the closest ATM or restaurant? The motivation behind the versatile administration supplier SP is to create and keep up the correspondence between the area server and the client. Every record portrays a POI, giving GPS directions to its area (xgps, ygps), and a portrayal or name about what is at the area. We sensibly accept that the versatile administration supplier SP is an inactive element and is not permitted to plot with the LS. We make this presumption on the grounds that the SP can focus the whereabouts of a cell phone, which, if permitted to connive with the LS, totally subverts any strategy or 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 portable

administration supplier to procure his/her coordinates. Since we are accepting that the portable 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 foe and tries to get more than he/she is permitted. Next we consider the case in which the area servers LS is the foe, and tries to exceptionally relate a client with a lattice coordinate.

ii. Security Model

Before we characterize the security of our convention, we present the idea of k out of N versatile careless exchange as takes after. Definition 1.•(k out of N versatile careless exchange (OTN k×1) [27]). OTN k×1 conventions contain two stages, for instatement what's more, for exchange. The introduction stage is controlled by the sender (Bob) who claims the N information components X1,X2, . . . ,XN. Weave normally figures a promise to each of the N information components, with an aggregate overhead of O(N). He then sends the responsibilities to the recipient (Alice). The exchange stage is utilized to transmit a solitary information component to Alice.

Toward the start of every exchange Alice has an information I, and her yield toward the end of the stage ought to be information component XI. An OTN k×1 convention backings up to k progressive exchange stages. Based on the above definition, our convention is formed of initialisation stage and exchange stage. We will now diagram the steps needed for the stages and afterward we will formally characterize the security of these phases.Our initialisation stage is controlled by the sender (server), who possesses a database of area information records and a 2- dimensional key grid Km×n, where m and n are lines and sections deferentially. A component in the key framework is referenced as ki,j.

Every ki,j in the key lattice remarkably scrambles one record. An arrangement of prime forces S = {pc1 1 , . . . , pcN N }, where N is the quantity of squares, is accessible to general society. Each component in S the pi is a prime and ci is a little regular number such that pci i is more prominent than the square size (where every square contains various POI records). We require, for comfort that the components of S take after an anticipated design. Moreover, the server sets up a typical security parameter k for the framework. Our exchange stage is built using six calculations: QG1, RG1, RR1, QG2, RG2, RR2. The initial three form the first and foremost stage (Oblivious Transfer Phase), while the last three form the second stage (Private Information Retrieval Stage).

III. RESULTS AND DISCUSSION

A. Protocol Description

We now depict our convention. We first give a convention rundown to contextualize the proposed arrangement and afterward depict the arrangement's convention in more detail.

Protocol Summary

A definitive objective of our convention is to acquire a situated (square) of POI records from the LS, which are near to the client's position, without bargaining the security of the client or the information put away at the server. We accomplish this by applying a two stage approach. The principal stage is in view of a two dimensional careless exchange [27] and the second stage is taking into account a communicationally effective PIR [12]. The negligent exchange based convention is utilized by the client to acquire the cell ID, where the client is placed, and the comparing symmetric key. The information of the cell ID and the symmetric key is then utilized as a part of the PIR based convention to get and unscramble the area information. The client decides his/her area inside a freely created network P by utilizing his/her GPS coordinates and structures an absent exchange query2. The base measurements of people in general network are characterized by the server and are made accessible to all clients of the framework. This open network superimposes over the secretly parcelled network created by the area server's POI records, such that for every cell Qi,j in the server's allotment there is no less than one Pi,j cell from people in general network. Since PIR does not oblige that a client is compelled to get stand out bit/obstruct, the area server needs to execute some assurance for its records. This is accomplished by encoding 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 decoding. This key is increased with the cell information recovered by the careless exchange inquiry. Consequently, regardless of the fact that the client utilizes PIR to get more than one record, the information

will be useless bringing about enhanced security for the server's database. Before we portray the convention in point of interest, we depict some initialisation performed by both sides.

B. Security Analysis

In this section, we dissect the security of the customer and the server. While the customer would not like to surrender the security of his/her area, the server would not like to reveal different records to the customer. This would not make much business sense in a mixture of utilizations. Our investigation will be regarding the security definitions in Area 2.3.

Client's Security

On a very basic level, the data that is most important to the client is his/her area. This area is mapped to a cell Pi,j. In both periods of our convention, the unaware exchange based convention and the private data recovery based convention, the server should not have the capacity to recognize two inquiries of the customer from one another. We will now depict both cases independently. In the unmindful exchange stage, every direction of the area is scrambled by the ElGamal encryption plan.

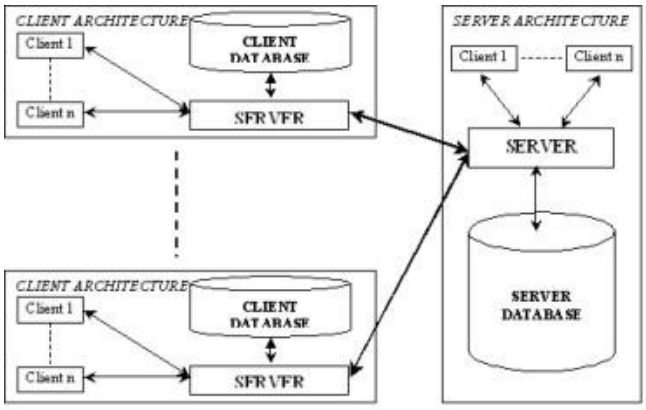

Figure 1: Architecture of Protection Privacy

Sever's Security

Naturally, the server's security obliges that the customer can recover one record just in every question to the server, and the server should not reveal different records to the customer in the reaction. Our convention attains to the server's security in the unaware exchange stage, which is based on the Naor-Pinkas unaware exchange convention [27]. Our Algorithm 1 is the same as the Naor-Pinkas unaware exchange convention with the exception of from the one-out-of-n unaware exchange convention, which is based on the ElGamal encryption plan.

C. **Performance**

We actualized our area built question arrangement 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.

Figure 2: User login page

Figure 2: Existing User Login

Figure 3: New User Registration

Figure 4: Protection privacy for user

IV. CONCLUSION

In this paper we have exhibited an area based question arrangement that utilizes two conventions that empowers a client to secretly focus and procure area information. The main step is for a client to secretly focus his/her area utilizing absent exchange on an open lattice. 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 exhibits that our convention is inside viable limits.

Future work will include testing the convention on numerous distinctive cell phones. The portable result we give may be not the same as 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. Also, the issue concerning the LS supplying misdirecting information to the customer is likewise intriguing. Protection saving notoriety methods appear to be a suitable way to address such issue. A conceivable arrangement could incorporate systems from [16]. Once suitable solid arrangements exist for the general case, they can be effectively coordinated into our methodology.

V. REFERENCES

[1] Russell Paulet, Md. Golam Kaosar, Xun Yi, and Elisa Bertino, Fellow, IEEE, "Privacy-Preserving and Content-Protecting Location Based Queries," IEEE Transaction on Knowledg and Data Engineering , vol. 26, No. 5, May 2014

[2] (2011, Jul. 7) Openssl [Online].Available:http:// www.openssl.org

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

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

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

[6] 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.

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

[8] 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.

[9] 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.

[10] 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.

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

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

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

[20] 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.

[21] 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.

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

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries," in Proc. CRYPTO, vol. 1666, Santa Barbara, CA, USA, 1999, pp. 791–791.

[28] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. EUROCRYPT, vol. 1592, Prague, Czech Republic, 1999, pp. 223–238.

[29] R. Paulet, M. Golam Kaosar, X. Yi, and E. Bertino, "Privacypreserving and content-protecting location based queries," in Proc. ICDE, Washington, DC, USA, 2012, pp. 44–53.

[30] B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with mix-zones over road networks," in Proc. ICDE, Hannover, Germany, 2011, pp. 494–505.

[31] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (corresp.)," IEEE Trans. Inform. Theory, vol. 24, no. 1, pp. 106–110, Jan. 1978.

[32] V. Shoup, (2011, Jul. 7). Number thoery library [Online]. Available: http://www.shoup.net/ntl

[33] L. Sweeney, "k-Anonymity: A model for protecting privacy," Int. J. Uncertain. Fuzziness Knowl. Based Syst., vol. 10, no. 5, pp. 557–570, Oct. 2002.

[34] T. Xu and Y. Cai, "Feeling-based location privacy protection for location-based services," in Proc. 16th ACM CCS, Chicago, IL, USA, 2009, pp. 348–357.