ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Study on User-Defined Privacy Grid System for Continuous Location-Based Service

Dr. Shaik Abdul Nabi
Professor,
Dept of CSE,
AVN Institute of Engineering and Technology.

G.Dayakar
Assistant Professor,
Dept of CSE,
AVN Institute of Engineering and Technology.

Golij Yuvadeep Kumar
PG Scholar,
Dept of CSE,
AVN Institute of Engineering and Technology.

ABSTRACT:

Location-based services (LBS) need users to unceasingly report their location to a doubtless untrusted server to get services supported their location, which may expose them to privacy risks. Sadly , existing privacy-preserving techniques for LBS have many limitations, like requiring a fully-trusted third party, giving restricted privacy guarantees and acquisition high communication overhead. During this paper, we have a tendency to propose a user-defined privacy grid system referred to as dynamic grid system (DGS); the primary holistic system that fulfills four essential needs for privacy-preserving shot and continuous LBS. (1) The system solely requires a semi-trusted third party, accountable for effecting easy matching operations properly.

This semi-trusted third party will not have any data a couple of user's location. (2) Secure shot and continuous location privacy is secured beneath our outlined adversary models. (3) The communication price for the user doesn't rely on the user's desired privacy level , it solely depends on the number of relevant points of interest within the section of the user. (4) though we have a tendency to solely target vary and k-nearest-neighbor queries in this work, our system is simply extended to support different spatial queries while not dynamic the algorithms go past the semi-trusted third party and also the information server, provided the desired search space of a spatial question is abstracted into spatial regions.

Experimental results show that our DGS is a lot of economical than the progressive privacy-preserving technique for continuous LBS.

KEYWORDS:

location privacy, cryptography, location-based services.

I.INTRODUCTION:

IN today's world of quality and present net connectivity, AN increasing variety of individuals use location-based services (LBS) to request data relevant to their current locations from a range of service suppliers(SPs). this will be the explore for close points of interest(POIs) (e.g., restaurants and hotels), location-aware advertising by firms, traffic data tailored to the route and direction a user is traveling and then forth. The use of LBS, however, will reveal way more a couple of person to potentially Teflon service suppliers than many folks would be willing to disclose. By chase the requests of a person it's doable to make a movement profile that can reveal data a couple of user's work (office location), medical records (visit to specialist clinics), philosophy (attending political events), etc. Nevertheless, LBS is terribly valuable and in and of itself users should be able to create use of them while not having to offer up their location privacy. Variety of approaches have recently been planned for conserving the user location privacy in LBS.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In general, these approaches are classified into 2 main classes. (1) Fully-trusted third party (TTP).The most in style privacy-preserving techniques need a TTP to be placed between the user and therefore the service supplier to hide the user's location data from the service supplier the third party is keeping track of the precise location of all users and blurring a querying user's location into a cloaked area that features k one different users to attain k-anonymity. This TTP model has 3 drawbacks. (a) All users ought to continuously report their precise location to the third party, even though they are doing not subscribe any LBS. (b) As the third party is aware of the precise location of each user, it becomes a horny target for attackers. (c) The k-anonymity-based techniques solely win low regional location privacy because cloaking a locality to incorporate k users in follow usually leads to tiny cloaking areas. (2) personal data retrieval (PIR) or oblivious transfer (OT). though PIR or OT techniques don't need a 3rd party, they incur a far higher communication overhead between the user and therefore thes ervice supplier, requiring the transmission of way more information than the user really desires Only a number of privacy-preserving techniques are proposed for continuous LBS [2], [7].

These techniques rely on a TTP to ceaselessly expand a cloaked space to include the ab initio allotted k users. These techniques not solely inherit the drawbacks of the TTP model, but they even have different limitations. (1) Unskillfulness. Ceaselessly expanding cloaked areas considerably will increase the query process overhead. (2) Privacy leak. Since the database server receives a collection of consecutive cloaked areas of a user at totally different timestamps, the correlation among the cloaked areas would offer helpful data for inferring the user's location. (3) Service termination. A user has to terminate the service once users an initio allotted to her cloaked space leave the system

II.RELATED WO-RK:

There square measure several researchers concentrating on the a way to obtain the privacy and accuracy in LBSs one amongst the researchers was Dewri, World Health Organization includes a long history within the field of privacy in location-based services. He has numerous publications with reference to achieving the privacy in LBSs His last paper [1] projected a user-controlled privacy experience "a user-centric location based mostly service architecture", wherever the user determines the required level of privacy supported his accuracy necessities. A provider "privacy-supportive LBS" provides supplemental information to the user for creating "informed" privacy decisions. The system can inform the user of the accuracy (or lack thereof) supported the privacy specifications input into the system, looking on "a service-similarity profile "which the user gets. If the user is happy with the result (even if it's errors or the privacy is beneath the desired level), they will opt to proceed with the question. If they are not happy, they will modification the privacy level into the balance of accuracy/privacy that's acceptable to them.

The main purpose of previous papers is to grasp (LBS) technology and known the key parts behind the service. Some papers gift a taciturn survey of location based services, the technologies deployed to trace the mobile user's location, the accuracy and reliableness associate with such measurements, and also the network parts deployed by the wireless network operators to modify these varieties of services. Different papers define the user necessities in terms of mobile device features and LBS applications. In addition to the overall plan of the LBS, the researchers discussed the impact on shopper, and utility computing offer enticing money and technological blessings. As an example, Zhang and Mao studied the results of 3individual level factors; consumption values, privacy, and subjective norms on consumers' intention to adopt location-based services on their mobile phones and to spread positive spoken (WOM) concerning LBS. Such knowledge helps business produce effective communications to attract a lot of potential adopters. In lightweight of the present findings, promoting communications have to be compelled to height en perceived consumption values concerning exploitation

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

LBS. All these scientific papers offer the attracted individuals a general plan concerning LBSs, and the way this service was important. Researchers have long been responsive to the potential privacy risks related to LBSs, as a result of they know whereas the user used one amongst these application services to retrieve the accuracy data, this new practicality comes with considerably exaggerated risks to non-public privacy. they need projected variety of promising these papers gift an outline of various protection goals and elementary location privacy approaches, as well as a classification of various sorts of attacks in line wit the applied offender data. They processed totally different protection goals and elementary location privacy while Dewri's matrix measurements was 320 × 320grid coated thirty two kms, wherever every cell reflects to a hundred × a hundred m space with 124.5 K information transferred.

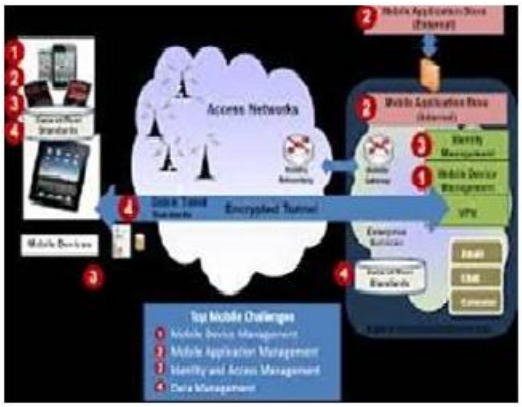

Fig.1.Architecture of DNS

This activity of each cell won't win the accuracy that the user is looking for, further as providing the user with unnecessary needed data. Figure three in contestable the main plan about the previous restriction. Suppose the user was in location (x, y) and his inquires was regarding some eating house or coffee, Dewri's system can give him a matrix regarding all the red spots, that is way from his interest. In fact, what he want is simply associate degree data regarding the closest neighbor from his location. As a result, we have a tendency to zoom this space to achieve the goal of accuracy whereas maintaining an equivalent amount of transmitted information, that's delineate within the parallelogram form in the same figure. The new similarity matrix used the main conception of Dewri's matrix 320 × 320 grid - wherever we have a tendency to will still in (124.5 KB) transferred information -, however every cell assimilates to ten × ten m space. This new cell can winthe accuracy and potency results for user

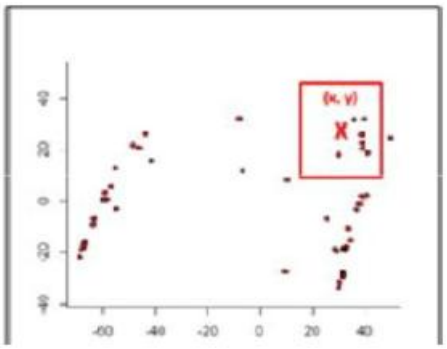

Fig.2.The New Region That the Similarity Matrix Should Covered

When the user search for a selected location around his space, the application can offer the user with the mandatory information he desires. With the arrival similarity matrix, the user location are exposed, therefore losing his privacy. So, the vital question comes here, however we'll preserve the America er location? This question target-hunting us to our second contribution. the solution to the present question can rely upon hiding the user location by creating the first location anonymous (x, y) to provide a brand new (x`, y`). The relationship between the coordinates exemplified in When the user search for a selected location around his space, the application can offer the user with the mandatory information he desires. With the arrival similarity matrix, the user location are exposed, therefore losing his privacy. So, the vital question comes here, however we'll preserve the Americaer location? This question target-hunting us to our second contribution. the solution to the present question can rely upon hiding the user location by creating the first location anonymous (x, y) to provide

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

a brand new (x`, y`). The relationship between the coordinates exemplified in

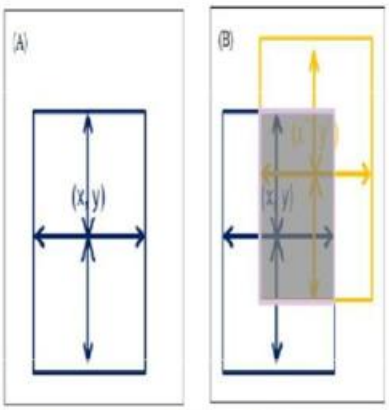

Fig-3: Anonymous User Location. (A) Clarified the Main Idea about Changing User Location. (B) The Intersection Area between Two Regions.

III.ADVERSARIAL MODELS

We currently discuss adversarial models relating to QS and SP, and then gift the formal security proof of our DGS in Section 4. A malicious QS or SP can attempt to break a user's privacy by operating with the info out there to them at intervals the delineate protocol. we tend to don't contemplate QS or SP with access to external info in a roundabout way associated with the protocol. User namelessness As delineate higher than, both QS and SP can attempt to de-anonymize a user by exploitation the information contained within the protocol (although they still faithfully follow the protocol itself). whereas QS doesn't have any info a couple of user that will permit it to narrow down the list of users that will match a particular query, SP has access to the plaintext question of a user. This query, however, solely contains the question region and also the grid parameters, and with the data out there, QS can therefore do no higher than establish that the user is somewhere at intervals the question region. One different concern relating to the de-anonymization of users is that if as an example the services of SP area unit paid services, then SP would possibly as an example be ready to link a question with a billing record and a minimum of establish the presence of a user in a query space.

whereas during this paper we tend to contemplate it acceptable that a user may be set to be at intervals a question region by QS(after all, the user will freely select the question space and hence select it specified her personal privacy necessities are met), there's different analysis which might permit to prevent the linking of a question space to a particular user through request records, as an example the work by Yau and An. therefore albeit the SP needs the authentication of users to a (paid) service, the service may be provided where as protecting the namelessness of the user. However, no matter in which means the SP provides the service, the privacy guarantees can continuously be higher than TTP, as a TTP continuously knows the precise location of the users, whereas in our system neither QS nor SP recognize the precise location of a user. Regarding paid services and QS, in such a case QS doesn't any info to slender down the geographic location of a user, albeit it's getting used as a paid service and can link queries to request records. Relating to the deanonymization of users, we tend to conjointly note that the kind of dish in a query sent to SP or the density of POIs per cell.

IV.CONCLUSION:

In this paper, we have a tendency to project a dynamic grid system for providing privacy-preserving continuous LBS. Our DGS includes the question server and therefore the service supplier, and cryptographic functions to divide the entire question process task into 2 elements that are performed individually by QS and SP. DGS doesn't need any fully-trusted third party; instead, we have a tendency to need solely the a lot of weaker assumption of no collusion between QS and SP. This separation conjointly moves the info transfer load far from the user to the cheap and high-bandwidth link between QS and SP. we have a tendency to conjointly designed economical protocols for our DGS to support each continuous k-nearest-neighbor and vary queries. to judge the performance of DGS, we have a tendency to compare it to the progressive technique requiring a TTP.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

DGS provides higher privacy guarantees than the TTP theme, and therefore the experimental results show that DGS is associate degree order of magnitude a lot of economical than the TTP theme, in terms of communication value. In terms of computation value, DGS conjointly forever out performs the TTP theme for NN queries; it's comparable or slightly dearer than the TTP theme for vary queries.

REFERENCES:

(1) B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymouslocation queries in mobile environments with PrivacyGrid,"in Proc. 17th Int. Conf. World Wide Web, 2008, pp. 237–246.

(2) C.-Y. Chow and M. F. Mokbel, "Enabling private continuousqueries for revealed user locations," in Proc. 10th Int. Conf. Adv.Spatial Temporal Databases, 2007, pp. 258–273.

(3) B. Gedik and L. Liu, "Protecting location privacy with personalizedk-anonymity: Architecture and algorithms," IEEE Trans.Mobile Comput., vol. 7, no. 1, pp. 1–18, Jan. 2008.

(4) M. Gruteser and D. Grunwald, "Anonymous usage of locationbasedservices through spatial and temporal cloaking," in Proc. 1stInt. Conf. Mobile Syst., Appl. Services, 2003, pp. 31–42.

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

(6) M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper:Query processing for location services without compromisingprivacy," in Proc. 32nd Int. Conf. Very Large Data Bases, 2006, pp. 763–774.

(7) T. Xu and Y. Cai, "Location anonymity in continuous locationbasedservices," in Proc. 15th Annu. ACM Int. Symp. Adv. GeographicInf. Syst., 2007, pp. 39:1–39:8.

(8) T. Xu and Y. Cai, "Exploring historical location data for anonymitypreservation in location-based services," in Proc. IEEE INFOCOM,2008, pp. 547–555.

(9) G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan,"Private queries in location based services: Anonymizers are notnecessary," in Proc. ACM SIGMOD Int. Conf.Manag. Data, 2008,121–132.

(10) M. Kohlweiss, S. Faust, L. Fritsch, B. Gedrojc, and B. Preneel,"Efficient oblivious augmented maps: Location-based serviceswith a payment broker," in Proc. 7th Int. Conf. Privacy EnhancingTechnol., 2007, pp. 77–94.

(11)R. Vishwanathan and Y. Huang, "A two-level protocol to answerprivate location-based queries," in Proc. IEEE Int. Conf. Intell. SecurityInformat., 2009, pp. 149–154.

(12) J. M. Kang, M. F. Mokbel, S. Shekhar, T. Xia, and D. Zhang,"Continuous evaluation of monochromatic and bichromaticreverse nearest neighbors," in Proc. IEEE 23rd Int. Conf. Data Eng.,2007, pp. 806–815.

(13) C. S. Jensen, D. Lin, B. C. Ooi, and R. Zhang, "Effective densityqueries of continuously moving objects," in Proc. IEEE Int. Conf.Data Eng., 2006, p. 71.

(14) S. Wang and X. S. Wang, "AnonTwist: Nearest neighbor queryingwith both location privacy and k-anonymity for mobile users,"in Proc. 10th Int. Conf. Mobile Data Manag.: Syst. Services Middelware,2009, pp. 443–448.

(15) W. B. Allshouse, W. B. Allshousea, M. K. Fitchb, K. H. Hamptonb,D. C. Gesinkc, I. A. Dohertyd, P. A. Leonebd, M. L. Serrea, andW. C. Millerb, "Geomasking sensitive health data and privacy: An evaluation using an E911 database,"

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Geocarto Int., vol. 25, pp. 443–452, Oct. 2010.

Author's Details:

Dr. Shaik Abdul Nabi is working as professor & Head of the Dept. of CSE, AVN Inst.Of Engg.& Tech, Hyderabad, T.S, India. He completed his B.E (Computer Science) from Osmania University, Hyderabad. He has completed his M.Tech. from JNTU Hyderabad campus and he received Doctor of Philosophy (Ph.D) in the area of Web Mining from AcharyaNagarjuna University, Guntur, AP, India. He is a certified professional by Microsoft. He is having 17 years of Teaching Experience in various Engineering Colleges. He has published 15 publications in International / National Journals and presented 08 papers in National / International conferences. His expertise areas are Data warehousing and Data Mining, Data Structures & UNIX Networking Programming, Cloud Computing and Mobile Computing.

G.Dayakar is working as Asst. Professor in Dept. of CSE, AVN Institute Of Engineering & Technology, Hyderabad, T.S, India. He completed his B.Tech (Computer Science) from JNTU, Hyderabad. He has completed his M.Tech. from JNTU Hyderabad campus, India. He is a certified professional in Teaching by National Institute Of Technical Teachers Training & Research (Govt Of India) He is having 10 years of Teaching Experience in various Engineering Colleges. His expertise areas are Design and Analysis Of Algortithms, Data Structures & UNIX Networking Programming.

Goli j Yuvadeep Kumar PG Scholar in Dept of CSE .AVN Institute of Engineering And Technology.