International Journal Of

Recent Scientific Research

ISSN: 0976-3031

Volume: 7(5) May -2016

AREA BASED ADMINISTRATIONS FOR DYNAMIC MATRIX FRAMEWORK

Rosy Yamini K M and Indira Gandhi.R

THE OFFICIAL PUBLICATION OF
INTERNATIONAL JOURNAL OF RECENT SCIENTIFIC RESEARCH (IJRSR)
http://www.recentscientific.com/ recentscientific@gmail.com

ISSN: 0976-3031

Available Online at http://www.recentscientific.com

International Journal of Recent Scientific Research
Vol. 7, Issue, 5, pp. 11177-11179, May, 2016

International Journal of Recent Scientific Research

Research Article

AREA BASED ADMINISTRATIONS FOR DYNAMIC MATRIX FRAMEWORK

Rosy Yamini K M and Indira Gandhi.R

G.K.M. College of Engineering and Technology, Chennai, Tamilnadu, India

ARTICLE INFO

Article History:

Received 06th February, 2015
Received in revised form 14th March, 2016
Accepted 23rd April, 2016
Published online 28th May, 2016

Keywords:

Dynamic grid systems, location privacy, location-based services. Cryptography.

ABSTRACT

Location-based casework (LBS) crave users to continuously address their breadth to a potentially untrusted server to achieve services based on their location, which can betrayal them to aloofness risks. Unfortunately, absolute privacy-preserving techniques for LBS have several restrictions such as acute a fully-trusted third party, alms bound aloofness guarantees and also with high communication. We adduce a user-defined aloofness filigree arrangement alleged activating filigree arrangement (DGS); the first holistic arrangement that fulfills four capital requirements for privacy-preserving snapshot and connected LBS. (1) The arrangement only requires a semi-trusted third party, amenable for accustomed out simple analogous operations correctly. This semi-trusted third affair does not accept any advice about a user's location. (2) Secure snapshot and connected breadth aloofness is affirmed beneath our defined adversary models. (3) The advice amount for the user does not depend on the user's adapted aloofness level, it alone depends on the number of accordant credibility of absorption in the around of the user. (4) Although we alone focus on ambit and k-nearest-neighbor queries in this work, our arrangement can be calmly continued to abutment added spatial queries after alteration the algorithms run by the semi-trusted third affair and the database server, provided the appropriate seek breadth of a spatial concern can be absent into spatial regions. Experimental after-effects appearance that our DGS is added able than the advanced privacy-preserving address for connected LBS.

INTRODUCTION

In today's apple of advancement and abiding Internet connectivity, an accretion amount of humans use location-based casework (LBS) to appeal advice accordant to their accepted locations from a variety of account providers. This can be the seek for nearby points of absorption (POIs) (e.g., restaurants and hotels), location aware commercial by companies, cartage advice tailored to the highway and administration a user is traveling and so forth. The use of LBS, however, can acknowledge abundant added about a being to potentially untrustworthy account providers than abounding humans would be accommodating to disclose. By tracking the requests of a being it is possible to body a movement contour which can acknowledge advice about a user's plan (office location), medical annal (visit to specialist clinics), political angle where LBS can be actual admired and as such users should be able to accomplish use of them after accepting to accord up their breadth privacy. A amount of approaches accept recently been proposed for attention the user breadth aloofness in LBS. These approach can be classified into two main categories.

Fully-trusted third affair (TTP). The lot of popular privacy-preserving techniques crave a TTP to be placed between the user and the account provider to adumbrate the user's location information from the account provider. The main task of the third affair is befitting clue of the exact breadth of all users and abashing a querying user's breadth into a buried area that includes k 1 added users to accomplish k-anonymity. This TTP model has three drawbacks.

1. All users accept to continuously report their exact breadth to the third party, even admitting they do not subscribe to any LBS.
2. As the third affair knows the exact breadth of every user, it becomes an adorable ambition for attackers.
3. The k-anonymity-based techniques alone accomplish low regional breadth aloofness because cloaking a arena to cover k users in conveyance usually after-effects in baby cloaking areas. (2) Private information retrieval (PIR) or absent alteration (OT). Although PIR or OT techniques do not crave a third party, they incur a abundant college advice aerial amid the user and the account provider, acute the manual of abundant more information than the user in fact needs. Only a few

**Corresponding author: Rosy Yamini K M*
G.K.M. College of Engineering and Technology, Chennai, Tamilnadu, India

privacy-preserving techniques accept been proposed for connected LBS. These techniques await on a TTP to continuously aggrandize a buried breadth to cover the initially assigned k users. These techniques not alone accede the drawbacks of the TTP model, but they as well accept added limitations.

Proposed System

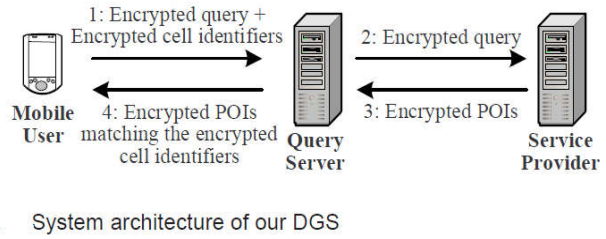
A user-defined confidentiality grid system called dynamic grid system (DGS) to deliver privacy-preserving Polaroid and continuous LBS. The main idea is to place a semi trusted third party, dubbed query server (QS), among the employer and the service provider (SP). QS only requirements to be semi-trusted because it will not save/stock or even have access to any user locality information. Semi-trusted in this context means that while QS will try to define the position of a user, it static correctly transmits out the modest matching operations required in the protocol. Untrusted QS would arbitrarily modify and drop messages also insert fake messages, which is why our system depends on semi-trusted QS.

The key indication of our DGS. In DGS, a querying user first determines a query area, where the user is comfortable to disclose the fact that she is someplace inside this query region. The query area is divided into equal-sized grid cells centred on the self-motivated grid organization stated by the user. Then, the user encodes a query that includes the information of the query region and the self-motivated grid structure, and encodes the identity of each grid cell intersecting the required quest region of the longitudinal query to yield a set of encoded identifiers. Next, the user sends a request including (1) the encoded query and (2) the encoded identifiers to QS, which is a semi-trusted party located between the user and SP. QS stores the encoded identifiers and onward he encrypted query to SP specified by the user. SP decrypts the query and selects the POIs inside the query region after its database.

Advantages of Proposed System

Aimed at both selected POI, SP encodes its evidence, using the dynamic grid structure specified by the user to find a grid cell covering the POI, and encodes the cell identity to produce the encrypted identifier for that POI. The encoded POIs with their consistent encoded identifiers are returned to QS. QS Stores the set of encrypted POIs and only returns to the user a subdivision of encoded POIs whose consistent identifiers match any one of the encoded identifiers primarily sent by the user. After the user receives the encoded POIs, she decrypts them to get their exact positions and calculates a query response.

System Architecture



System architecture of our DGS

Fig 1 system design of DGS

List of modules

Mobile users

Each mobile user is equipped with a GPS-enabled device that determines the user's location in the procedure (xu, yu). The user can achieve Polaroid or continuous LBS from our system by issuing a latitudinal query to a individual SP complete QS. Our system services the user select a query area for the spatial query, such that the user is enthusiastic to divulge to SP the fact that the user is located in the given area. Then, a grid structure is created and is entrenched inside an encoded query that is promoted to SP, it will not reveal any information about the query region to QS itself. In accumulation, the statement cost for the user in DGS does not depend on the query area size. This is unique of the strategic structures that distinguish DGS from the existing techniques based on the fully-trusted third party model.

Service providers (SP)

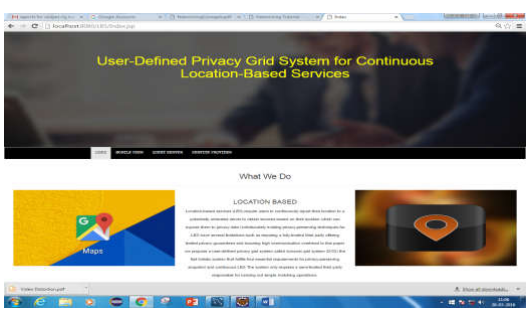
Our system supports any number of independent service providers. Each SP is a latitudinal database administration system that stocks the location information of a particular type of static POIs, e.g., restaurants or hotels, or the collection location information of a individual company, e.g., Starbucks or McDonald's. The spatial database uses an present latitudinal index (e.g., R-tree or grid structure) to index POIs and answer range queries (i.e., retrieve the POIs placed in a confident area). SP does not communicate with mobile users directly, but it runs services for them incidentally complete the query server (QS).

Query servers (QS)

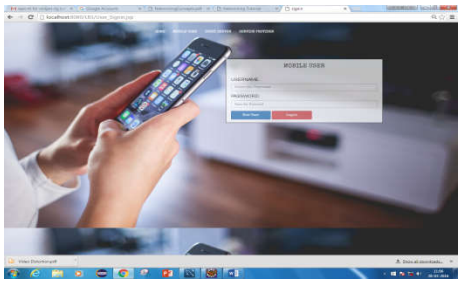
QS is a semi-trusted event placed between the portable user and SP. Similar to the most popular infrastructure in present privacy-conserving techniques for LBS, QS can be sustained by a telecom operator . 1) The mobile user sends a request that includes (a) the personality of a user-specified SP, (b) an encoded query (which includes information about the user-defined grid structure), and (c) a set of scrambled identifiers (which are calculated based on the user-defined grid structure) to QS. 2) QS stores the encrypted identifiers and forwards the encrypted query to the user-specified SP. 3) SP decrypts the query and finds a proper set of POIs from its database. It then encrypts the POIs and their corresponding identifiers based on the grid structure specified by the user and sends them to QS. 4) QS returns to the user every scrambled POI whose scrambled identifier matches one of the encrypted identifiers initially sent by the user. The user decrypts the received POIs to build a candidate answer set, and then performs a simple filtering process to clip false positives to total an exact query answer.

Screen Shorts

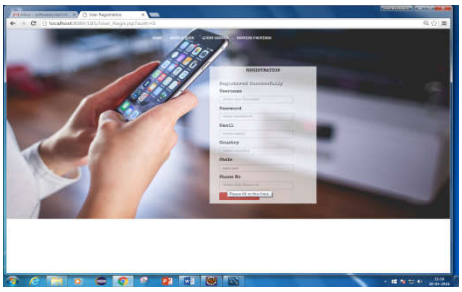
Home page



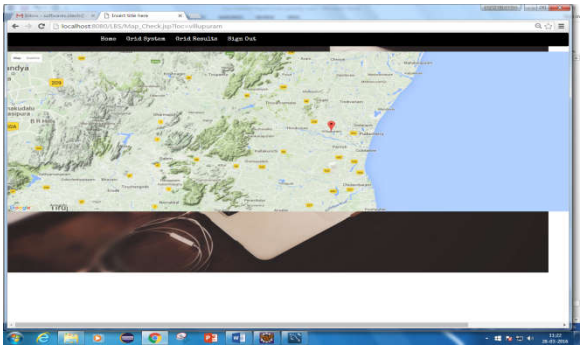
Mobile user



User registration



Location



CONCLUSION

In this paper, we projected a dynamic grid system (DGS) for providing privacy-preservative continuous LBS. Our DGS contains the query server (QS) and the service provider (SP), and cryptographic utilities to divide the whole query processing task into two parts that are executed individually by QS and SP. DGS does not include any fully-trusted third party (TTP); instead, we require only the far weaker statement of no permission between QS and SP. This departure also moves the data transmission load away from the user to the inexpensive and high-bandwidth link between QS and SP. We also considered efficient protocols for our DGS to support both continuous k-nearest-neighbour (NN) and range queries. To evaluate the performance of DGS, we associate it to the state-of-the-art technique requiring a TTP. DGS offers better privacy promises than the TTP scheme, and the experimental results show that DGS is an order of scale more well-organized than the TTP scheme, in terms of communication price. In terms of computation price, DGS also always overtakes the TTP scheme for NN queries; it is similar or slightly more expensive than the TTP scheme for range queries.

References

1. B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with PrivacyGrid," in WWW, 2008.
2. C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations," in SSTD, 2007.
3. B. Gedik and L. Liu, "Protecting location privacy with personalized kanonymity: Architecture and algorithms," IEEE TMC, vol. 7, no. 1, pp. 1–18, 2008.
4. M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in ACM MobiSys, 2003.
5. P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," IEEE TKDE, vol. 19, no. 12, pp. 1719–1733, 2007.
6. M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," in VLDB, 2006.
7. T. Xu and Y. Cai, "Location anonymity in continuous location-based services," in ACM GIS, 2007.
8. "Exploring historical location data for anonymity preservation in location-based services," in IEEE INFOCOM, 2008.
9. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in ACM SIGMOD, 2008.
10. M. Kohlweiss, S. Faust, L. Fritsch, B. Gedrojc, and B. Preneel, "Efficient oblivious augmented maps: Location-based services with a payment broker," in PET, 2007.
11. R. Vishwanathan and Y. Huang, "A two-level protocol to answer private location-based queries," in ISI, 2009.
12. J. M. Kang, M. F. Mokbel, S. Shekhar, T. Xia, and D. Zhang, "Continuous evaluation of monochromatic and bichromatic reverse nearest neighbors," in IEEE ICDE, 2007.
13. C. S. Jensen, D. Lin, B. C. Ooi, and R. Zhang, "Effective density queries of continuously moving objects," in IEEE ICDE, 2006.
14. S. Wang and X. S. Wang, "AnonTwist: Nearest neighbor querying with both location privacy and k-anonymity for mobile users," in MDM, 2009.
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, and W. C. Millerb, "Geomasking sensitive health data and privacy protection: an evaluation using an E911 database," Geocarto International, vol. 25, pp. 443–452, October 2010.
16. A. Gkoulalas-Divanis, P. Kalnis, and V. S. Verykios, "Providing kanonymity in location based services," SIGKDD Explor. Newsl., vol. 12, pp. 3–10, November 2010.

****

TSSN 0976-3031