International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October 2016

Continuous Location Based Services for User Defined Privacy Grid System

[1]THATIKANTI KARTHIK, [2]B. VENKANNA.
1.PG Scholar, Department of CSE, sphoorthy engineering college, Hyderabad
2.M-tech, Assistant professor, Department of CSE, sphoorthy engineering college, Hyderabad

ABSTRACT:

Location-based services (LBS) requires users to constantly position reports is likely to be unreliable for location-based services, which may jeopardize the privacy of the server. Unfortunately, the techniques of preserving the privacy of LBS has many restrictions, such as requiring a completely reliable third party, and offers few guarantees of privacy and incurring high above the connection. In this paper, we propose Privacy distribution network knowledge by the user called bio-network system (DGS), the first totalitarian regime manages four basic conditions for a cat to maintain privacy and LBS continuous. (1) The system requires only one-third of medium trust, is responsible for implementing a simple matching operations correctly. Is this a trusted third party has almost no information on where the user is present. (2) is guaranteed safe for a cat and privacy site continuously in our models specific discount. (3) The cost of the call the user does not depend on the privacy required for the user level, it just depends on the amount of corresponding points in the vicinity of the user area. (4) despite the fact that we focus only on the scale investigations and closest in this paper neighbor, our system can be easily expanded to support queries and other algorithms without spatial changes managed by trusted third parties almost started and the server database, provided that the required surface for the spatial query can extract the spatial regions. The results showed that our DGS is the most effective method of prior art LBS Privacy happening.

INTRODUCTION:

In today's world of movement and until now never connect to the Internet, A growing number of people use location-based services (LBS) To request information relevant to its current location A variety of service providers. This could be a search for a relative Points of Interest (POI) (eg restaurants and hotels), location aware Declaration of business, designed for traffic information Roads and address that the user is traveling, and so on. Utilization LBS,

however, can reveal much about a person is likely to Service Providers did not trust many people are willing Detected. By tracing requests a person could have been To build a moving image that can reveal information about User Action (office location) and medical records (a visit to a specialist Clinics), political views (to attend political events), etc. However, LBS can be very useful and as such users You should be able to take advantage of them without having to give site's privacy. There are a number of methods have recently The proposal to maintain the privacy of the user's geographic location in the pound. In general, these approaches can be classified into two main Categories. A third (1) full confidence (TTP). The most popular Techniques necessary to maintain the privacy of the Pakistani Taliban that are placed between the The user and the service provider to hide the user's location Information service provider (eg [1] - [8]). Home third task is to track the exact location of all The users blurred site user query and wrapped areathat includes k - 1 to other users to achieve k-anonymity. The Pakistani Taliban Model has three disadvantages. (A) to all users constantly Informing the exact location of a third party, although I do not agree on any lbs. (B) as a third person knows The exact location of each user becomes an attractive target for the The attackers. k-anonymity (C) based techniques, achieve only low Regional location privacy due to the blocking zone to include K Users in practice usually results in small areas of coverage. (2) Private Information Retrieval (bear) or foreign transfer (OT). in spite of PIR techniques or do not need a third OT, incurred by the party Communications load is much greater between the user and service provider, which requires transfer so much About user really needs (eg [9] - [11]). It has been proposed only a handful of techniques privacy Continuously LBS [2], [7]. These techniques are based on the Pakistani Taliban Continue to expand the area involved include in the beginning User as assigned. These techniques not only inherits the negative Pakistani Taliban model, but also has other restrictions. (1) incompetence. Continued expansion of the areas many sides Increases query processing overhead. (2) Leakage privacy. Because the server database receives a group of wrapped in a row User areas in different time stamp, and the relationship between Hooded areas provide useful information to infer User location. (3) termination. The user can

cancel Service when users who were hired at the beginning of his leave the area involved System. In this paper, we propose Knowledge Network System Privacy bio-network system (DGS) is called for the provision of privacy Continuous capture and LBS.

REVIEW:

The main idea is to semitrusted A third, called a query server (QS), between the user And service provider (SP). QS only have to be a semi-reliable Because not collect / store or even get to any user Location information. In this context, it means that the confidence semi-whileQS attempt to locate the user's presence is still correctly It performed a simple operation that coincide required in the protocol, That is, it does not modify or drop any messages or create new messages. The QS is reliable and drop messages arbitrarily modified as And injection of false messages, and that is why our system depends Semi-QS reliable. The main idea of our DGS. In Dubai Gold Shares, the user can check first Specify the query area where the user is comfortable to detect The fact that somewhere in this consultation area. Question The area is divided into cells of equal size of the network based on dynamic Network structure selected by the user. Then the user encrypts The query that includes information from a query area and network structure vital, and encrypt the identity of each network Cells intersecting the search area required for spatial query Producing a set of coded identifiers. Then the user sends Application, including (1) a query encryption and (2) Encrypted Identifications of QS, which is a trusted party to the semi sandwiched between User and SP. QS stores coded IDs and forward Consultation encrypted user-defined LS. SP decrypts Check and identify the important points in the field of your database query. Each selected point of interest, SP your information is encrypted, using Exact dynamic network structure by the user to find the grid cell PDI cover, and encrypt the cell to produce identity Encrypted ID to this important point. PDI are encrypted with the Coded identifiers corresponding QS returned. QS stores A number of important points are encrypted and only returns the user to a subset of the encrypted important points corresponding to any of the corresponding identifiers Posted coded identifiers from the beginning by the user. After the user Receive important points

encrypted, they decrypt it to get exactly Sites and calculates the answer to the query. Because the user is constantly scouring may need Information on points of interest in other cells of the network (Consultation) area that have not been requested by QS. User So simply sends coded identifiers required cells QS network. Since QS pre-stored in the important points of the Along with the identifiers consulting your own encrypted area, it does It is not necessary to gather Syrian pounds to help. necessary simply because QS The important points that correspond to any of the newly coded ID Encrypted user ID required. After the user has received QS PDI encrypted, the query can be evaluated locally. When the deregistration of a user query with QS, QS eliminates Have POIs stored encrypted encryption identifiers. Further, When the search area required for consultation through space

Area outside the current query, the user can deregister consultation with QS and new re-consultation with a new area of inquiry issues. Contributions. We DGS contains the following main features:

(1) No Taliban Pakistanis. We DGS requires only consultation semi reliable server (QS) (any reliable way to properly operate the protocol) between Users and service providers.

(2) Site privacy. DGS Ensures QS and other users are not able to infer any information Consultation on location, and user service provider SP can only conclude that the user is somewhere within user specified Check the region as long as QS and SP are not complicit.

(3) low over the connection. The cost of communication DGS user does not depend on the specific query by the user The size of the region. Only it depends on a number of important points in the grid cells Intertwined with the search area requires a query. (4) for expansion For various spatial queries. DGS applies to different types of Spatial queries without changing the algorithms performed by QS SP or if your answers can be extracted spatial regions, for example, NN Eks- consultations [12] and the density of investigations [13].

EXISTING SYSTEM:

- Spatial cloaking techniques have been widely used to preserve user location privacy in LBS. Most of the existing spatial cloaking techniques

rely on a fully-trusted third party (TTP), usually termed *location* anonymizer that is required between the user and the service provider.

- When a user subscribes to LBS, the location anonymizer will blur the user's exact location into a cloaked area such that the cloaked area includes at least k – 1 other users to satisfy k-anonymity.
- In a system with such *regional location privacy* it is difficult for the user to specify personalized privacy requirements. The feeling based approach alleviates this issue by finding a cloaked area based on the number of its visitors that is at least as popular as the user's specified public region. Although some spatial clocking techniques can be applied to peer-to-peer environments, these techniques still rely on the k-anonymity privacy requirement and can only achieve regional location privacy.
- Furthermore, these techniques require users to trust each other, as they have to reveal their locations to other peers and rely on other peers' locations to blur their locations, another distributed method was proposed that does not require users to trust each other, but it still uses multiple TTPs.
- Another family of algorithms uses incremental nearest neighbor queries, where a query starts at an "anchor" location which is different from the real location of a user and iteratively retrieves more points of interest until the query is satisfied. While it does not require a trusted third party, the approximate location of a user can still be learned; hence only regional location privacy is achieved.

DISADVANTAGES OF EXISTING SYSTEM:

- The TTP model has four major drawbacks.
- It is difficult to find a third party that can be fully trusted.
- All users need to continuously update their locations with the location anonymizer, even when they are not subscribed to any LBS, so that the location anonymizer has enough information to compute cloaked areas.

- Because the location anonymizer stores the exact location information of all users, compromising the location anonymizer exposes their locations.
- k-anonymity typically reveals the approximate location of a user and the location privacy depends on the user distribution.

PROPOSED SYSTEM:

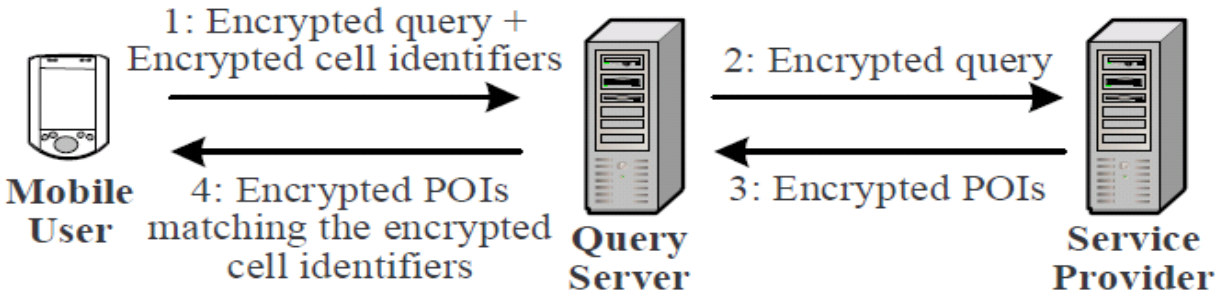
- In this paper, we propose a user-defined privacy grid system called *dynamic grid system* (DGS) to provide privacy-preserving *snapshot* and *continuous* LBS.
- The main idea is to place a semi trusted third party, termed *query server* (QS), between the user and the service provider (SP). QS only needs to be semi-trusted because it will not collect/store or even have access to any user location information.
- *Semi-trusted* in this context means that while QS will try to determine the location of a user, it still correctly carries out the simple matching operations required in the protocol, i.e., it does not modify or drop messages or create new messages. An untrusted QS would arbitrarily modify and drop messages as well as inject fake messages, which is why our system depends on a semi-trusted QS.
- **The main idea of our DGS.** In DGS, a querying user first determines a *query area*, where the user is comfortable to reveal the fact that she is somewhere within this query area. The query area is divided into equal-sized grid cells based on the dynamic grid structure specified by the user. Then, the user encrypts a query that includes the information of the query area and the dynamic grid structure, and encrypts the identity of each grid cell intersecting the required search area of the spatial query to produce a set of encrypted identifiers.
- Next, the user sends a request including (1) the encrypted query and (2) the encrypted identifiers to QS, which is a semi-trusted party located between the user and SP. QS stores the encrypted identifiers and forwards he encrypted query to SP specified by the user. SP decrypts the

query and selects the POIs within the query area from its database.

ADVANTAGES OF PROPOSED SYSTEM:

- For each selected POI, SP encrypts its information, using the dynamic grid structure specified by the user to find a grid cell covering the POI, and encrypts the cell identity to produce the encrypted identifier for that POI.
- The encrypted POIs with their corresponding encrypted identifiers are returned to QS. QS stores the set of encrypted POIs and only returns to the user a subset of encrypted POIs whose corresponding identifiers match any one of the encrypted identifiers initially sent by the user.
- After the user receives the encrypted POIs, she decrypts them to get their exact locations and computes a query answer.

SYSTEM ARCHITECTURE:



System architecture of our DGS

CONCLUSION

In this paper, we proposed a dynamic grid system (DGS) for providing privacy-preserving continuous LBS. Our DGS includes the query server (QS) and the service provider (SP), and cryptographic functions to divide the whole query processing task into two parts that are performed separately by QS and SP. DGS does not require any fully-trusted third party (TTP); instead, we require only the much weaker assumption of no collusion between QS and SP. This separation also moves the data transfer load away from the user to the inexpensive and high-bandwidth link between QS and SP. We also designed efficient protocols for our DGS to support both continuous k-nearest-neighbor (NN)

and range queries. To evaluate the performance of DGS, we compare it to the state-of-the-art technique requiring a TTP. DGS provides better privacy guarantees than the TTP scheme, and the experimental results show that DGS is an order of magnitude more efficient than the TTP scheme, in terms of communication cost. In terms of computation cost, DGS also always outperforms the TTP scheme for NN queries; it is comparable 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, andW. 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.

[17] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *CRYPTO*, 2001.

[18] A. Menezes, M. Qu, and S. Vanstone, "Some new key agreement protocols providing mutual implicit authentication," in *SAC*, 1995.

[19] S. Yau and H. An, "Anonymous service usage and payment in servicebased systems," in *IEEE HPCC*, 2011, pp. 714–720.

[20] M. Balakrishnan, I. Mohomed, and V. Ramasubramanian, "Where's that phone?: Geolocating ip addresses on 3G networks," in *ACM SIGCOMM IMC*, 2009.

[21] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: the secondgeneration onion router," in *USENIX Security*, 2004.

[22] G. Bissias, M. Liberatore, D. Jensen, and B. Levine, "Privacy vulnerabilities in encrypted HTTP streams," in *PET*, 2006.

[23] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *Pervasive Computing*, 2009.

[24] IEEE, *P1363-2000: Standard Specifications for Public-Key Cryptography*, 2000.

[25] A. B. Lewko and B. Waters, "Efficient pseudorandom functions from the decisional linear assumption and weaker variants," in *ACM CCS*, 2009