



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

A Location Based Queries for Securing Content and Assuring Privacy with Dynamic Grid System

Dr.V.Goutham¹, A. Narender², P. Sravani³

Professor, Dept. of CSE, TKREC, Telangana, India ¹

Assistant Professor, Dept. of CSE, TKREC, Telangana, India ²

M.Tech, Dept. of CSE, TKREC, Telangana, India ³

ABSTRACT: Location-based services (LBS) require users to unceasingly report their location to a possibly untrusted server to obtain services based on their location, which can expose them to privacy risks. Inappropriately, existing privacy-preserving techniques for LBS have several limitations, such as requiring a fully-trusted third party, offering limited privacy guarantees and incurring high communication overhead. In this paper, we propose a user-defined privacy grid system called dynamic grid system (DGS); the first holistic system that accomplishes four vital necessities for privacy-preserving snapshot and continuous LBS. The system only needs a semi-trusted third party, responsible for carrying out simple matching operations correctly. This semi-trusted third party does not have any information about a user's location. Secure snapshot and incessant location privacy is guaranteed under our defined adversary models. The communication cost for the user does not depend on the user's desired privacy level; it only depends on the number of relevant points of interest in the vicinity of the user. Although we only focus on range and k-nearest-neighbour queries in this work, our system can be easily protracted to support other spatial queries without changing the algorithms run by the semi-trusted third party and the database server, provided the required search area of a spatial query can be abstracted into spatial regions.

KEYWORDS: Dynamic grid systems, location privacy, location-based services, spatio-temporal query processing, cryptography.

I. INTRODUCTION

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 the encrypted query to SP specified by the user. SP decrypts the query and selects the POIs within the query area from its database. 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.

II. EXISTING SYSTEM

LBS can be very valuable and as such users should be able to make use of them without having to give up their location privacy. A number of approaches have recently been proposed for preserving the user location privacy in LBS.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

In general, these approaches can be classified into two main categories. Fully-trusted third party (TTP). The most popular privacy preserving techniques require a TTP to be placed between the user and the service provider to hide the user's location information from the service provider. The main task of the third party is keeping track of the exact location of all users and blurring a querying user's location into a cloaked area that includes $k-1$ users to achieve k -anonymity. (2) Private information retrieval (PIR) or oblivious transfer (OT). Although PIR or OT techniques do not require a third party, they incur a much higher communication overhead between the user and the service provider, requiring the transmission of much more information than the user actually needs.

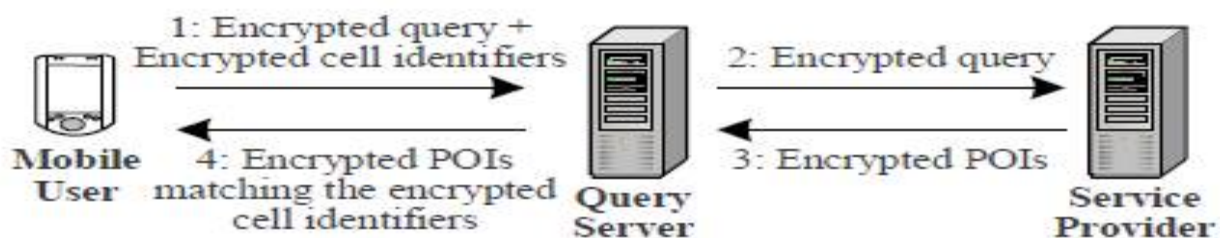
III. PROPOSED SYSTEM

This process proposes 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. 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.

IV. IMPLEMENTATION

4.1 User module

In this module the user can obtain snapshot or continuous LBS from our system by issuing a spatial query to a particular SP through QS. Our system helps the user select a query area for the spatial query, such that the user is willing to reveal to SP the fact that the user is located in the given area. Then, a grid structure is created and is embedded inside an encrypted query that is forwarded to SP, it will not reveal any information about the query area to QS itself. In addition, the communication cost for the user in DGS does not depend on the query area size. This is one of the key features that distinguish DGS from the existing techniques based on the fully-trusted third party model.



4.2 Query Server module

QS is a semi-trusted third party placed between the mobile user and SP. QS only needs to be semi-trusted because it will not collect/store or even have access to any user location information. 1) The mobile user sends a request that includes (a) the identity of a user-specified SP, (b) an encrypted query (c) a set of encrypted identifiers to QS. 2) QS stores the encrypted identifiers and forwards the encrypted query to the user-specified SP. 3) QS returns to the user every encrypted POI whose encrypted identifier matches one of the encrypted identifiers initially sent by the user. The user decrypts the received POIs to construct a candidate answer set, and then performs a simple filtering process to prune false positives to compute an exact query answer.

4.3 Service Provider

Module Each SP is a spatial database management system that stores the location information of a particular type of static POIs, e.g., restaurants or hotels, or the store location information of a particular company, e.g., Starbucks or

International Journal of Innovative Research in Computer and Communication Engineering

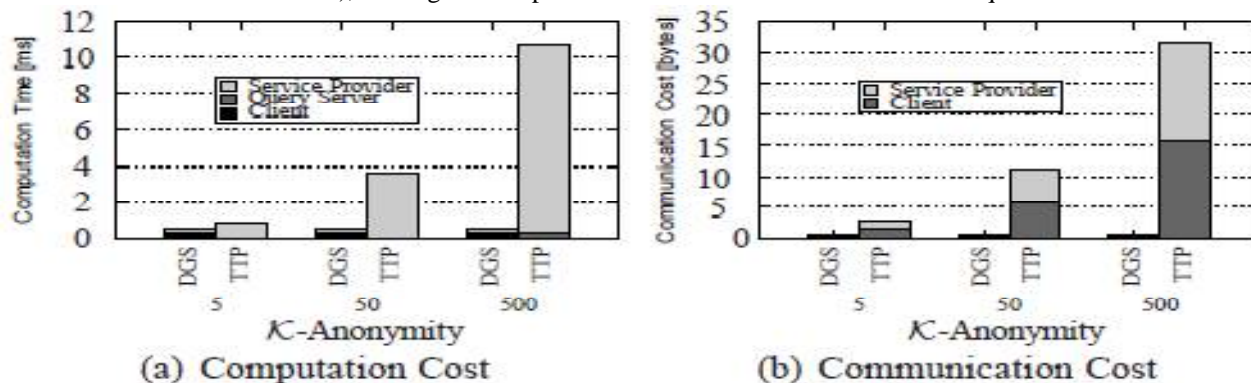
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

McDonald's. The spatial database uses existing spatial index to index POIs and answer range queries SP does not communicate with mobile users directly, but it provides services for them indirectly through the query server (QS).

V. EXPERIMENTAL RESULTS

In this section, we evaluate the performance of our DGS for both continuous range and k-NN queries through simulations. **Baseline algorithm.** We implemented a continuous spatial cloaking scheme using the *fully-trusted third party model* (TTP) [2]. TTP relies on a fully-trusted location anonymizer, which is placed between the user and the service provider (SP), to blur a querying user's location into a cloaked area that contains the querying user and a set of $K - 1$ other users to satisfy the user specified K-anonymity privacy requirement. To preserve the user's continuous location privacy, the location anonymizer keeps adjusting the cloaked area to contain the querying user and the $K - 1$ users. A privacy-aware query processor at SP returns a set of candidate POIs to the querying user through the location anonymizer [6], [2]. Then, the querying user computes an exact query answer from the candidate POIs. We compare our DGS with the TTP scheme for both continuous range and k-NN queries. We chose TTP as the baseline algorithm to compare against, as it is architecturally most similar to our DGS approach in that both systems require third-party servers to perform the main computation of the respective algorithm (although DGS only requires a semi-trusted third party). Other approaches such as private information retrieval (PIR) or oblivious transfer (OT) are fundamentally different and put a much higher burden in terms of complexity of the computation on the user's side. They typically also compare unfavourably against TTP and our DGS in terms of communication bandwidth required (an important attribute in mobile environments), making the comparison between TTP and DGS the most equivalent one.



VI. CONCLUSION & FUTURE WORK

In this Paper we proposed a dynamic grid system (DGS) for providing privacy-preserving continuous LBS. 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. 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. For the future enhancement we will expand this system by giving the location snapshot to share to the friend. In any emergency cases we will provide guest users module in case user did not register themselves in to the system.

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 k-anonymity: 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.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

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. Allshouse, 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.
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. Mohamed, and V. Ramasubramanian, "Where's that phone?: Geolocating ip addresses on 3G networks," in *ACM SIGCOMM IMC*, 2009.

BIOGRAPHY

Dr V. Goutham is a Professor and Head of the Department of Computer Science and Engineering at TEEGALA KRISHNA REDDY ENGINEERING COLLEGE affiliated to J.N.T.U Hyderabad. He received Ph.d from Acharya Nagarjuna University and M.Tech from Andhra University. He worked for various MNC Companies in Software Testing and Quality as Senior Test Engineer. His research interests are Software Reliability Engineering, software testing, software Metrics, and cloud computing.

Mr. A. Narender is working as a Assistant Professor in the Department of Computer Science and Engineering at TEEGALA KRISHNA REDDY ENGINEERING COLLEGE affiliated to J.N.T.U Hyderabad

Mrs.P.Sravani Department of Computer Science and Engineering at TEEGALA KRISHNA REDDY ENGINEERING COLLEGE affiliated to J.N.T.U Hyderabad.

.