Volume 6, Issue 3, March 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

UDCLBS::User Defined Privacy Grid System for Continuous Location Based Services

A.N.V.Supraja[1], G.Gopi Chand[1], B.N.V.Anusha[1], M.Lokesh[1], Y.ChittiBabu[2]
[1] UG Scholar, [2] Associate Professor
[1, 2] Department of Computer Science & Engineering, St.ANN'S College of Engineering & Technology, Chirala, Andhra Pradesh, India

Abstract: Location-based services (LBS) require users to continuously report their location to a potentially untrusted server to obtain services based on their location, which can expose them to privacy risks. Unfortunately, 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 fulfills four essential requirements for privacy-preserving snapshot and continuous LBS. (1) the system only requires 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. (2) Secure snapshot and continuous location privacy is guaranteed under our defined adversary models. (3) 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. (4) Although we only focus on range and k-nearest-neighbor queries in this work, our system can be easily extended 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. Experimental results show that our DGS is more efficient than the state-of-the-art privacy-preserving technique for continuous LBS.

Key Words: SQL Server, ASP.net, Mobile Computing

I. INTRODUCTION

In today's world of mobility and ever-present Internet connectivity, an increasing number of people use location-based services (LBS) to request information relevant to their current locations from a variety of service providers. This can be the search for nearby points of interest (POIs). The use of LBS, however, can reveal much more about a person to potentially untrustworthy service providers than many people would be will- ing to disclose. 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. In general, these approaches can be classified into two main categories. (1) 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 (e.g., [1]–[8]). 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 are that includes k−1 other users to achieve k-anonymity.

This TTP model has three drawbacks. (a) All users have to continuously report their exact location to the third party, even though they do not subscribe to any LBS. (b) As the third party knows the exact location of every user, it becomes an attractive target for attackers. (c) The k-anonymity-based techniques only achieve low regional location privacy because cloaking a region to include k users in practice usually results in small cloaking areas. (2) Private information retrieval (PIR) or oblivious transfer (OT). . In this project, 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 messag**es.**

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 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

II. RELATED WORK

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.[5]

III. PROPOSED WORK

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. 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.

IV. PROCEDURE FOR 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 distinguishes 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.

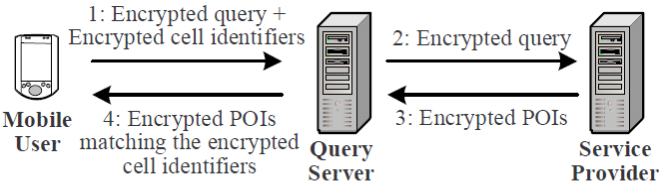
3) QS returns to the user every encrypted POI whose encrypted identifier matches one of the encrypted iden- tifiers initially sent by the user. The user decrypts the received POIs to construct a candidate answer set, and then performs a simple filtering process to prune false positives to compute an 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 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).

4.3.1 System Architecture



System architecture of our DGS

V. RESULTS & DISSCUSSIONS

5.1 Main Page: This is our main page for user

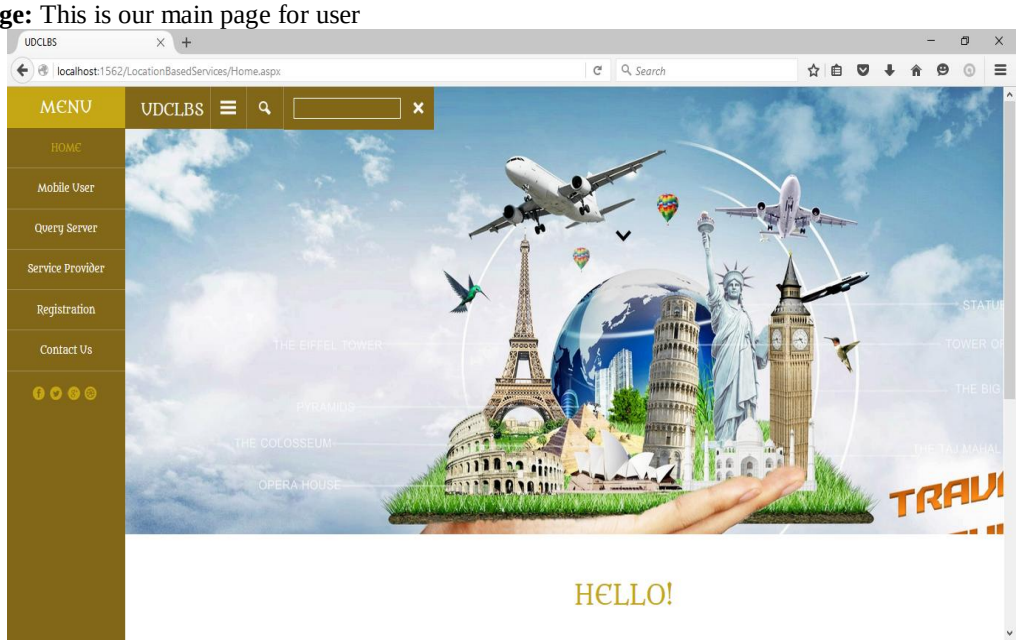


Fig 5.2: Registration Page: In this page user can register their details

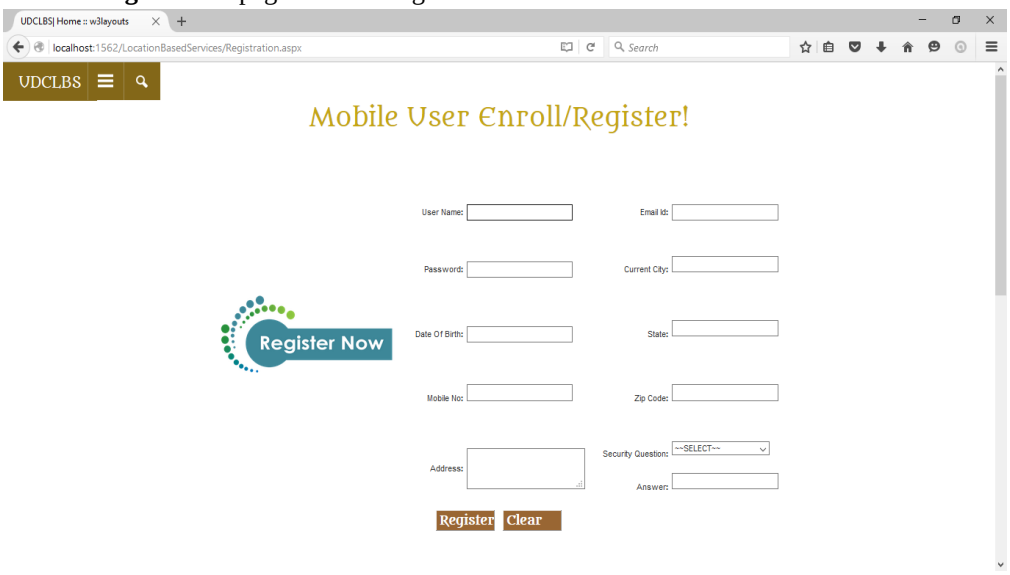


Fig 5.3: Login Page: In this page user can login with their ID and Password

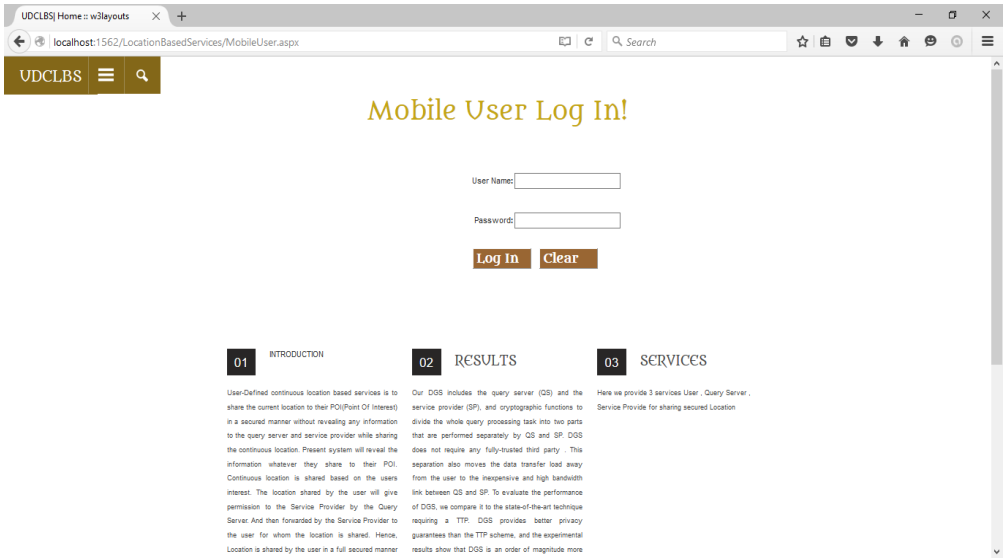


Fig 5.4: Share Location Page: In this user can share location.

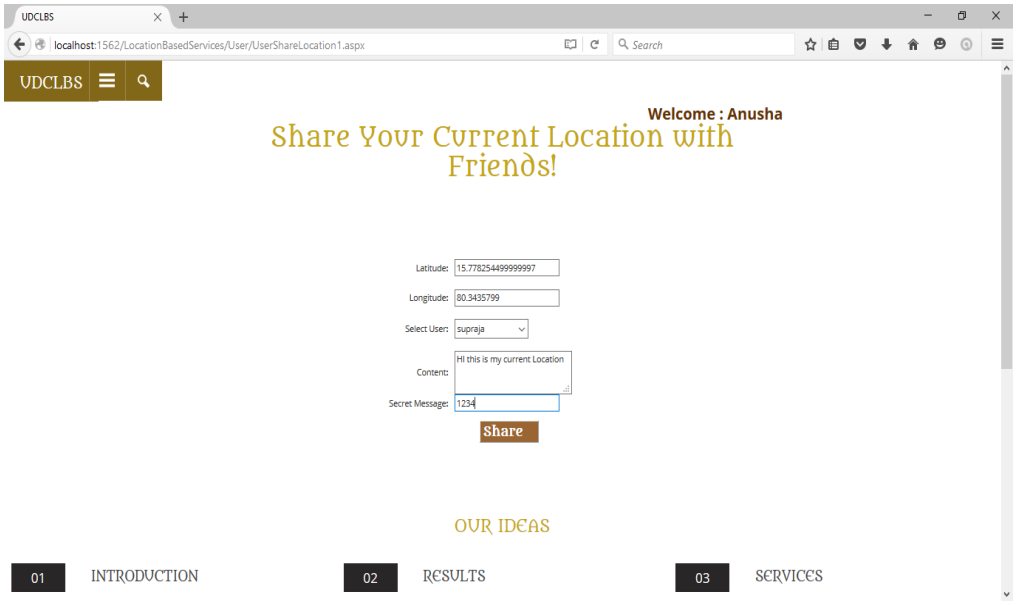
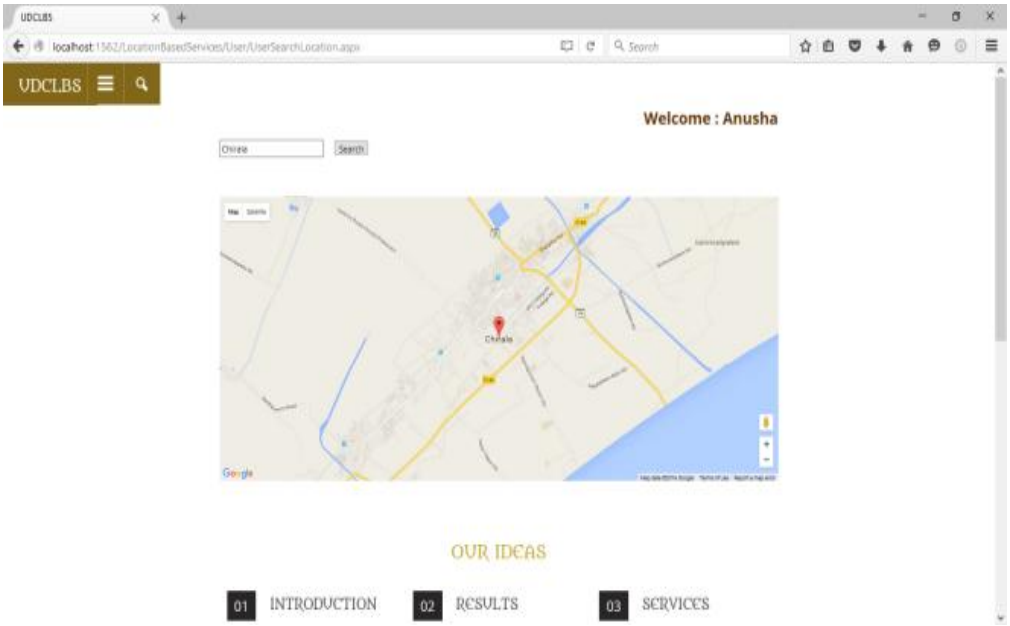


Fig 5.5: Search Location Page



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 pro- cessing 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] G. Ghinita, P. *Kalnis*, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Pri- vate queries in location based services: Anonymizers are not necessary," in ACM SIGMOD, 2008.
[9] 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.
[10] R. Vishwanathan and Y. Huang, "A two-level protocol to answer private location-based queries," in ISI, 2009.
[11] 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.
[12] C. S. Jensen, D. Lin, B. C. Ooi, and R. Zhang, "Effective density queries of continuously moving objects," in IEEE ICDE, 2006.
[13] S. Wang and X. S. Wang, "AnonTwist: Nearest neighbor querying with both location privacy and k-anonymity for mobile users," in MDM, 2009.
[14] 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.
[15] A. Gkoulalas-Divanis, P. Kalnis, and V. S. Verykios, "Providing k- anonymity 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.
[16] A. Menezes, M. Qu, and S. Vanstone, "Some new key agreement protocols providing mutual implicit authentication," in SAC, 1995.
[17] S. Yau and H. An, "Anonymous service usage and payment in service- based systems," in IEEE HPCC, 2011, pp. 714–720.
[18] M. Balakrishnan, I. Mohomed, and V. Ramasubramanian, "Where's that phone?: Geolocating ip addresses on 3G networks," in ACM SIGCOMM IMC, 2009.
[19] A.Veeraswamy," An Implementation of Efficient Data mining Classification Algorithm using Nbtree" International Journal of Computer Applications (0975 –8887) Volume 67–No.12, April 2013

