International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-144 PAGE NO: 856-863

Using DGS Preserving Location Based Services by Encryption privacy

POTHULA ANUSHA[1]& MD RAFEEQ[2]
[1]PG SCHOLAR Dept.CSE CMR TECHNICAL CAMPUS HYDERABAD, TS, INDIA and Email: - pothula.anusha21@gmail.com
[2]ASSOCIATE PROFESSOR Dept.CSE CMR TECHNICAL CAMPUS HYDERABAD, TS, and INDIA Email: - mdrafeeqcse@gmail.com

Abstract— Due to the large increasing use of Location Based Services (LBS), which require personal data of the user to provide the continuous service, protecting the privacy of these data has become a challenge. An approach to preserving a privacy is through anonymity, by hiding the identity and user location data of the mobile device from the service provider(third party) or from any unauthorized party who has access at the user's request .Considering the challenge mentioned, in this paper gives a classification according to the Architecture, approaches and techniques used in previous works, and presents a survey of solutions to provide anonymity in LBS including the open issues or possible improvements to current solutions. All of this, in order to provide guidelines for choosing the best solution approach to a specific scenery in which anonymity is required.

Keywords: Dynamic grid system, cloaking areas, location based services, Encryption, privacy.

1. Introduction

The consumer market for location-based services (LBS) is estimated to grow from 2.9 billion dollars in 2010 to 10.4 billion dollars in 2015. While navigation applications are currently generating the most significant revenues, locationbased advertising and local search will be driving the revenues going forward. The legal landscape, unfortunately, is unclear about what happens to a subscriber's location data. The nonexistence of regulatory controls has led to a growing concern about potential privacy violations arising out of the usage of a location-based application. While new regulations to plug the loopholes are being sought, the privacy conscious user currently feels reluctant to adopt one of the most functional business models of the decade. Privacy and usability are two equally important requirements for successful realization of a location-based application. Privacy (location) is looselydefined as a "personally" assessed restriction on when andwhere someone"s

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-144 PAGE NO: 856-863

position is deemed appropriate fordisclosure. To begin with, this is a very dynamic concept.Usability has a twofold meaning: a) privacy controls should beintuitive yet flexible, and b) the intended purpose of anapplication is reasonably maintained. Towards this end, priorresearch has led to the development of a number of privacycriteria, and algorithms for their optimal achievement.

However, there is no known attempt to bring into view the mutual interactions between the accuracy of a location coordinate and the service quality from an application using those coordinates. Therefore, the question of what minimal location accuracy is required for a LBS application to function remains open. The common man‟s question is: “how important is my position to get me to the nearest coffee shop?” which unfortunately remains unanswered in the scientific community. It is worth mentioning that a separate line of research in analyzing anonymous location traces has revealed that user locations are heavily correlated, and knowing a few frequently visited locations can easily identify the user behind a certain trace. The privacy breach in these cases occurs because the location to identity mapping results in a violation of user anonymity. The proposal in this work attempts to prevent the reverse mapping from user identity to user location in a user-controllable manner.

The term Location-Based Services (LBS) is a recent concept that denotes applications integrating with the general notion of services. Examples of such applications include emergency services, car navigation systems, tourist tour planning, or information delivery. In the modern environment each and every users has lots and lots of queries to analyze the locations in a global place, in that case the main motivate of server is to successfully serve the response to all the requestor without any delay as well as maintain the privacy of individuals. The basic idea of every server is the concept of load balancing; here the server requires reducing the number of queries submitted by mobile clients and query load on the server. However, mobile clients suffer from longer waiting time for the server to compute valid regions.

2. Private Information Retrieval (PIR) OR Oblivious Transfer (OT).

In paper [19] the authors find the problem of protecting location privacy of the mobile user to an Oblivious transfer problem, where the issuer of the request receives only its corresponding reply and

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-144 PAGE NO: 856-863

the service provider remains oblivious of the location of the user. Further on, they design some solutions based on different kinds of Oblivious Transfer (OT) namely Adaptive OT (implementing blind signatures), Dynamic OT and Proxy OT. They propose the solutions but do not provide any further analysis on the correctness or feasibility of their proposals. Based on [19], the authors in [20] propose an improved protocol by using two oblivious transfers where no third party is required to enable user's privacy. They assume the existence of a total server, which is responsible of a group of LBS providers. The user has to perform a double OT implemented with blind signatures in order to get the key required response to the query. This solution is thought for LBS that require payment.

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.

3. Dynamic Grid System

3.1 Spatial Cloaking

This technique is the most commonly used for protecting user location data from the third party attackers where in this technique extracted user location is blurred before submitting into service provider server for processing The solution proposed in this area is further classified by the architectural approach.

3.2 Semi Trusted Third Party (Dynamic Grid System)

To overcome the problem of in the above architecture propose a new architecture called dynamic grid system (DGS) [4] 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. QS only needs to be semi-trusted because it will not collect/ store or even have access to any user location information.

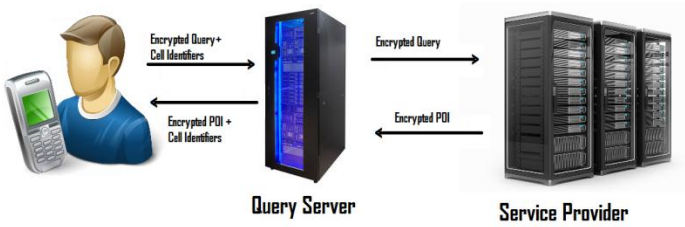


Fig: 1. Architecture

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

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-144 PAGE NO: 856-863

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

Algorithm for DGS

Input: User location (x, y), POI data P
Output: User's POI Query data U(P).
Initialization:
i. User Select POI Type P(t), QS Query Server, SP Service Provider.
ii. User set location, defined x, y (Current exact Location).

let $x_u,y_u \in$ U,
Map.getBounds(x_u,y_u)
return(x_b,y_b), (x_t,y_t) where b- bottom, t- top
Key Derivation Function KDF()
returns *k* (random key)
Enc(query) = IBE(P(t), k, (x_b,y_b), (x_t,y_t)) // At User side
Enc(query), User data of U ***fwd to***QS.
Create ID for Query and ***fwd*** Enc(query) to SP
Decrpt(query) at SP,
get (x_c,y_c)= Map.getCenter((x_b,y_b), (x_t,y_t));
while data != nulll
get POI P ∈ P(t),
sort based on dist,
create Query Set U(p).
end while
return Query Set U(p) to QS
At QS, fwd Query Set to User
Decrpt(query set U(P)) at USer,

3.3 Identity Based Encryption (IBE)

For an effective key management system these are all requirements 2] Authenticate users and decrypt data 3] Manage keys with partners 4] Deliver keys to trusted infrastructure components 5] Recover keys

Adi Shamir, one of the pioneers of public key cryptography, proposed a new type of public key algorithm in 1984. While public key systems have the inherent problem of distributing public keys and tying those public keys to a specific receiver. The scheme has chosen cipher text security in the random oracle model assuming a variant of the computational Diffie-

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-144 PAGE NO: 856-863

Hellman problem. This system is based on bilinear maps between groups.

In this paper we propose a fully functional identity-based encryption scheme. The performance of our system is comparable to the performance of ElGamal encryption. The security of our system is based on a natural analogue of the computational Diffie-Hellman assumption. this assumption showed that the new system has chosen cipher text security in the random oracle model. Using standard techniques from threshold cryptography [23, 24] the PKG in our scheme can be distributed so that the master-key is never available in a single location.

comparisons table

Parameter	Existing System (TTP)	Proposed System (DGS)
Computation Cost(Number of POIs)	0.6	1.4
Communication Cost(Number of POIs)	1000	10000
Computation Cost Number of Users (thousands)	0.8	0.6
Communication Cost Number of Users (thousands)	0.1	25
K-Anonymity Computation Cost	0.2	10
K-Anonymity Communication Cost	0.1	10

4. Results

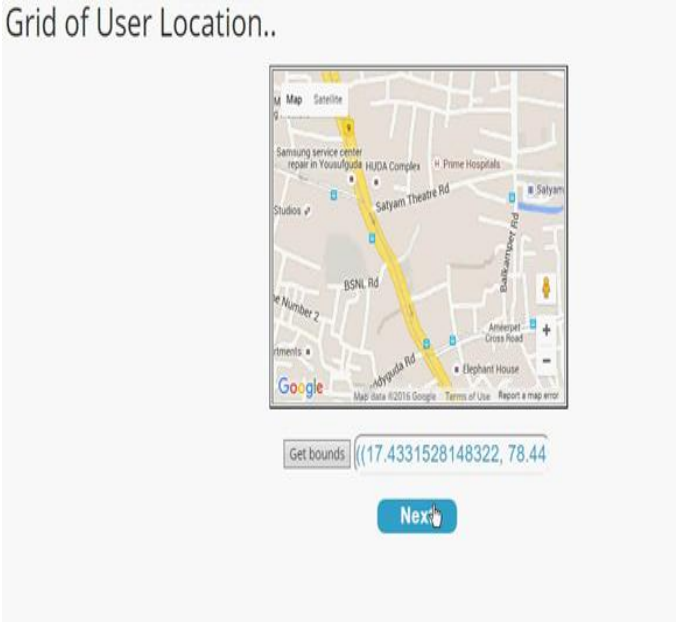
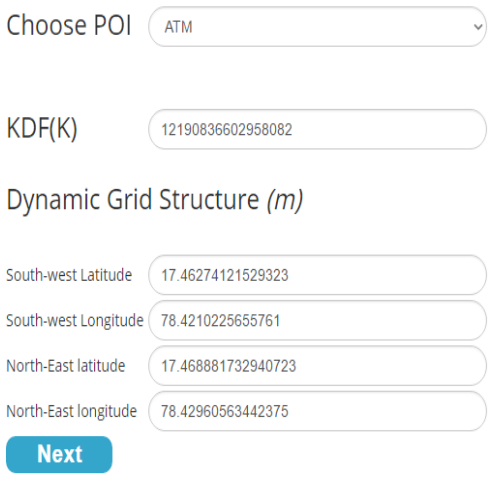


Fig.2 . Grid of user location preparation.



International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-144 PAGE NO: 856-863

Fig. 3. Preparation of Query

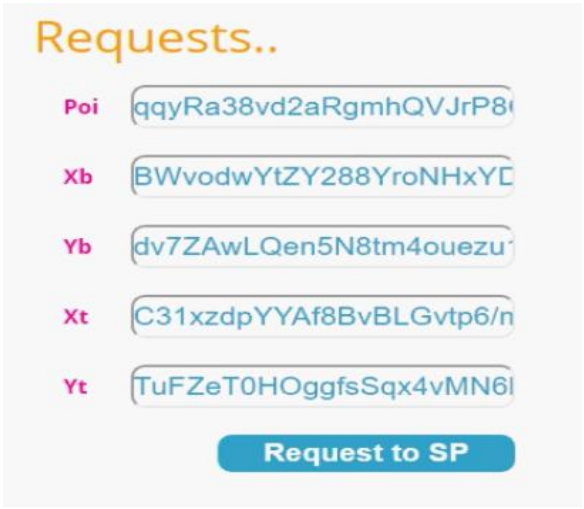


Fig 4. Encrypted Query forward to SP at QS

POI ID	POI Name	POI Type	City	Distance	Map
poi4	Sajid Enclave	Hotel	Hyderabad	3.44425883484452 km	View
poi3	CT Hotel	Hotel	Hyderabad	3.95463817359276 km	View
poi6	Begumpet Hotel	Hotel	Hyderabad	6.316447305152062 km	View
poi5	Malar Hotel	Hotel	Hyderabad	7.959666170513984 km	View

Fig. 5. POI results got at User.

5. Conclusion

It is necessary to propose new models that address new threats and attack models, which seek to break user's privacy in Location Based Services. These new models need to overcome the disadvantages of existing ones. Novel solutions approaches could combine different proposed solutions, to compensate the disadvantages of certain models with the advantages of others.

The job of updating or proposing a new survey will remain as an open task, as the development of new solutions to protect user's privacy in Location Based Services remains active; moreover it is necessary to classify the solutions by the privacy degree they offer, the attack model(s) from which they are resilient and the type of LBS to which they can be applied.

6. REFERENCES

[1] Schiller, J. Voisard, A.: Location-Based Services. Morgan Kaufmann Publishers (2004)

[2] Mohaisen, A., Hong, D., Nyang, D.: Privacy in Location based services: Primitives toward the solution. NCM (2008)

[3] C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations," in Proc. 10th Int. Conf. Adv. Spatial Temporal Databases, 2007, pp. 258–273.

[4] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity:

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-144 PAGE NO: 856-863

Architecture and algorithms," IEEE Trans. Mobile Comput., vol. 7, no. 1, pp. 1–18, Jan. 2008.

[5] M. Gruteser and D. Grunwald, "Anonymous usage of locationbased services through spatial and temporal cloaking," in Proc. 1st Int. Conf. Mobile Syst., Appl. Services, 2003, pp. 31–42.

[6] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," IEEE Trans. Knowl. Data Eng., vol. 19, no. 12, pp. 1719–1733, Dec. 2007.

[7] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query processing for location services withoutcompromising privacy," in Proc. 32nd Int. Conf. Very Large Data Bases, 2006, pp. 763–774.

[8] T. Xu and Y. Cai, "Location anonymity in continuous locationbased services," in Proc. 15th Annu. ACM Int. Symp. Adv. Geographic Inf. Syst., 2007, pp. 39:1–39:8.

[9]. Kido, H., Yanagisawa, Y., Satoh, T. An Anonymous Communication Technique using Dummies for Location-based Services. In: IEEE International Conference on Pervasive Services ICPS (2005) 88–97

[10]. Lu, H., Jensen, C.S., Yiu, M.L.: PAD: Privacy-Area Aware. Dummy-Based Location Privacy in Mobile Services MobiDE (2008) 16–23

[11]. Bamba, B., Liu, L., Pesti, P., Wang, T.: Supporting anonymous location queries in mobile environments with privacy grid. In: Proceedings of the International World Wide Web Conference, WWW (2008)

[12]. Gedik, B.,Liu, L.: Protecting location privacy with personalized k-anonymity: Architecture and algorithms. In: IEEE Transactions on Mobile Computing, TMC (2008) 1–18

[13]. Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of the International Conference on Mobile Systems,Applications, and Services, MobiSys (2003)

[14] Roman Schlegel, *Member, IEEE,* Chi-Yin Chow, *Member, IEEE,* Qiong Huang, *Member, IEEE,* and Duncan S. Wong, *Member, IEEE,* "User-Defined Privacy Grid System for Continuous Location-Based Services", IEEE Transactions on Mobile Computing, 2015.

[15]. Ardagna, C. A., Cremonini, M., Damiani, E., De Capitani di Vimercati S., Samarati, P.: Location privacy protection through obfuscation based

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-144 PAGE NO: 856-863

techniques. Data and Applications Security XXI, Volume 4602 (2007)

[16]. Wightman, P.M.; Jimeno, M.A; Jabba, D.; Labrador, M.: Matlock: A location obfuscation technique for accuracy-restricted applications. 2012 IEEE Wireless Communications and Networking Conference (WCNC) (2012)

[17]. Di Pietro, R., Mandati, R., Verde, N.V.: Track me if you can: Transparent obfuscation for Location based Services. 2013 IEEE 14th International Symposium and Workshops on World of Wireless, Mobile and Multimedia Networks (WoWMoM) (2013)