International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 20 Issue 3 – MARCH 2016.

SPATIAL – RSASSOL: IMPROVISED STRING SEARCH ON LOCATION ORIENTED SERVICES IN GRID SYSTEM

S.Preethika[1],P.Kanimozhi[2]

[1]*Student, Department of Computer Science and Engineering, I.F.E.T College of Engineering, Villupuram-605602, India*
[2]*Associate professor, HOD, Department of Computer Science and Engineering, I.F.E.T College of Engineering, Villupuram-605602, India*

preethiarshan@gmail.com
chandrankani@gmail.com

***Abstract*- In the modern world, mobile devices have grabbed much attention among the mobile users. Mobile devices are widely eminent for its easy retrieval of the searched records. To easily retrieve the information, the queries should be in clear and precised form. Several techniques were available on the study of location based services. Still, they lag behind the performance of searching the data using spatial data queries in Euclidean space. In privacy perspective, the aggregation of user defined queries is not incisively portraying the privacy. This paper intends to search the spatial data with the given appropriate queries in location based services using the novel RSASSOL Algorithm.The RSASSOL algorithm targets to gather and aggregate the nearest neighbor queries without compromising the privacy protection. Several distance-based range queries are situated as user-defined queries to heighten the protection of privacy. The spatial data exist in the spatial network, so as to improve a masking model, is designed. With our algorithm, the location-based users can efficiently protect their data and easily retrieve the search data. Through extensive simulations, the performance metrics such as feasibility, efficiency and accuracy of our approaches will be demonstrated.**

***Keywords*: Mobile devices, Location based services, Distance-based range queries, Spatial Data and RSASSOL algorithm.**

I. INTRODUCTION

With the fast advances in mobile communications innovations and proceeded with decreased price of location tracking devices, Location based services (LBSs) are generally perceived as an imperative element without bounds configuring the environment [8]. In spite of the fact that LBSs give numerous new open doors, the capacity to find portable clients likewise shows new dangers − the interruption of location security [7, 12]. Thelocation security is characterized as the capacity to anticipate the unapproved parties from realizing one's present or past area. Locationsecurity alludes to the danger that an enemy can acquire unapproved access to the crude region information, inferred then again registered area data by finding a transmitting gadget, capturing the area transmission channel and distinguishing the subject utilizing the gadget [13]. For instance, location data can be utilized to spam the clients with an undesirable commercials or to find out about clients' medicinal conditions, disagreeable political or religious perspectives.

Protection is a genuine security risk that can be to a great destructive to both organizations and buyers in the mobile environment. The location based assault can be performed either utilizing the mobile systems or database. By recovering the Point Of Interest (POIs) from the database server, the client can get solutions to different location based queries, which incorporate in finding the closest ATM machine, gas station, hospital or police headquarters. There are expanding mobile clients around the world. A considerable measure of research has been done on privacy preserving. However, nobody gave supreme certification of user's information and inquiry. Essentially, when client utilized particular location based administration or enlisted for that, then LBS can give number of different administrations such as conveyance coupons or other advertising data to client who is in a particular topographical zone. These days, there are number of client exploits location based services and its sub-relation is increasing.

II. RELATED WORK

The k-anonymity is a way to deal with security insurance was first created for securing the distributed medicinal information [19]. K-anonymity ensures the failure of the adversary to recognize an individual record in any event k−1 different records. [6, 15] give solution for ideal k-anonymization. Personalization of protection prerequisites has pulled in consideration in recent years [10, 20]. Other related work incorporates anonymization of high dimensional relations [4] and augmenting the idea of k-anonymization by means of l-diversity [17], t-closeness [16] and m-invariance [21]. The idea of area k-anonymity was presented in [12] where k is set to be uniform for all clients. The idea of customized area k-anonymity with adjustable QoS particulars, initially presented in [10], is embraced by a few others [18,

11]. Most well known answers for location privacy [12, 10, and 18] host embraced the trusted third party anonymization model, which has been effectively conveyed in different ranges, for example, Web browsing [1].

Two delegate ways to deal with customized location anonymization are the CliqueCloak estimation presented in [10] and the Casper framework [18]. The CliqueCloak estimation depends on the capacity to find a section in a graph to perform location shrouding, which is costly and demonstrates poor execution for expansive k. The Casper methodology performs the location anonymization utilizing the quadtree-based pyramid information structure, permitting quick shrouding. Nonetheless, because of the coarse determination of the pyramid structure and absence of instruments to guarantee the QoS and oblige the span of the shrouding location, the shrouding zones in Casper are much bigger than would normally be appropriate, prompting poor QoS by the clients.

As opposed to the trusted outsider anonymizer model, two or three exploration projects, with Prive [11] being the most agent one, endeavor to evacuate the trusted outsider anonymizer by depending on a decentralized associate to the companion model and the presence of a trusted incorporated centralized server. The primary specialized test in this work includes dynamic development of close-by associate groupings that can perform local anonymization for one another. In truth, the Privacy Grid methodology can be effectively adjusted to such settings to perform the real area shrouding among the chosen peers.

III. PROPOSED WORK

RSASSOL ALGORITHM

For RSAS queries, the spatial solution is based on the Dijkstra's algorithm. Given a query point q, the query range radius r, and a string predicate, we expand from q on the road network using the Dijkstra's algorithm until the destined points are obtained. The distance r away from q and verify the string predicate either in a post-processing step or on the intermediate results of the expansion. The performance degrades quickly when the query range enlarges and/or the data on the network increases.

This motivates us to find a novel method to avoid the unnecessary road network expansions, by combining the pruning's from both the spatial and the string predicates simultaneously. For ESAS queries, our experimental evaluation covers both synthetic and real data sets of up to 10 million points and 6 dimensions. We partition a road network G = {V,E} into m edge disjoint sub-graphs G_1,G_2, . . . ,G_m, where m is a user parameter, and build one string index (Filter Tree) for strings in each sub-graph. We also select a small subset VR of nodes from V as reference nodes: they are used to prune candidate points/nodes whose distances to the query point q are out of the query range r. The proposed architecture is given below:

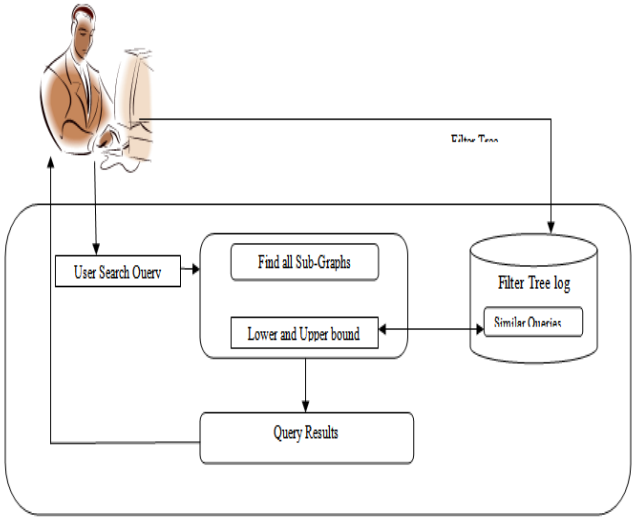

Fig.1. Working of RSASSOL algorithm

The RSASSOL algorithm is presented as follows:

1. Obtain the queries for string search.
2. Discovering the subgraphs for the given queries.
3. Filter tree approach is used as sub-graphs that display and output the similarity points of the actual queries string.
4. Lower and upper bound of candidate points is calculated and it is pruned from the distance of the candidates.
5. The above step 4 is repeated until the string predicate is estimated.
6. The accurate distance for every candidate points to the query points that returns the optimal distances for the specified query string.

Selectivity estimation of range queries on street systems is a much more difficult issue than its complement in the Euclidean space. In any case, they are just ready to gauge the quantity of nodes and edges in the range. None can be proficiently adjusted to gauge the number of focuses in the range. One best solution is introducing so as to focuses as hubs in the system more edges. This unmistakably builds the space utilization altogether since the quantity of focuses is much bigger than the quantity of existing hubs. At that point,it likewise has the difficulties of coordinating the spatial selectivity estimator with the string selectivity estimator in a successful route, as in the Euclidean space. The distance figured and put away in capacity model between a hub to all reference hubs, which permits us to figure lower and upper distance limits for any given hub and any destination.

IV. EXPERIMENTAL RESULTS

To test RSAS queries, we utilize two road systems datasets NAN and CAN from Digital Chart of the World server. Then, we consider the adequacy of the RSASSOL calculation for RSAS inquiries in this location. Firstly, we examine the impact of determination and the quantity of reference hubs, and the quantity of subgraphs worked by the RPar estimation, in the preprocessing venture, to the RSASSOL estimation. The effects of reference hubs determination on the queries execution exists in two folds. To begin with, various determination procedures will wind up in selecting different reference hubs. The advanced planar estimation is dependably the best system, given the same number of reference hubs. Second, the quantity of reference hubs is also critical. After that we contemplate the impact of number of subgraphs, on the running time of RSASSOL. In any case, having more subgraphs additionally implies more access to smaller FilterTrees, which presents queries overhead when scanning for estimated strings.

In range query information, the base operation of all records is recovered inside of the range of upper and lower limits. The Data structures for range queries are Range tree is the information structure utilized for sorting out the range inquiries. Range inquiry operation includes in preprocessing the information onto the information structure and to recover the effective responses for the inquiries by taking any subset as the basic information. Edit distance is a measuring procedure of how two unique strings are to each other and ascertains the least operations for changing a string. Edit distance operation likewise find the programmed spell checks rectifications and decide the applicant required corrections if there is any incorrectly spelled words which has low distance to the word in the tree.

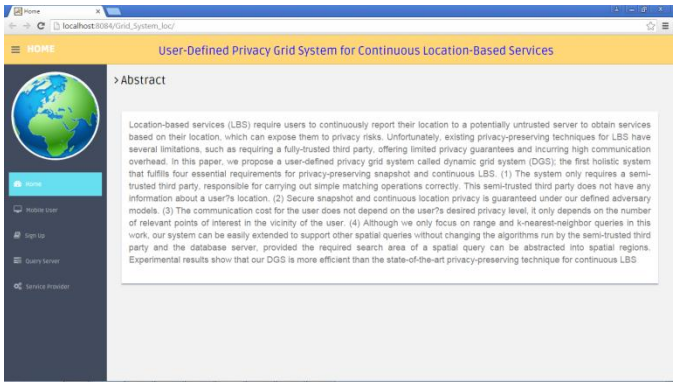

Fig.2. Home Page of User Defined Privacy System

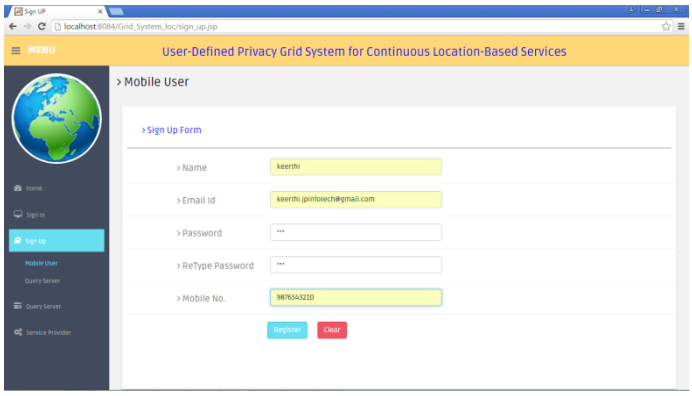

Fig.3. Registration with mobile user.

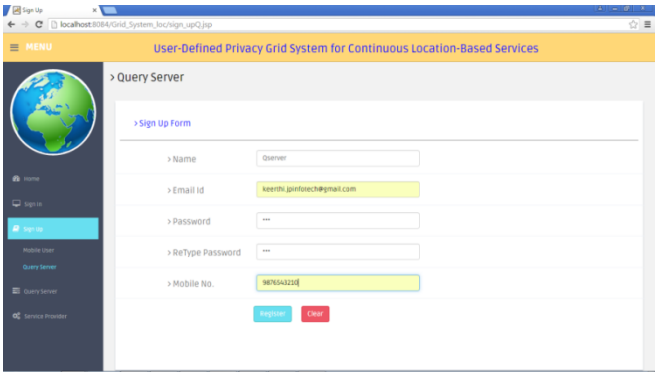

Fig.4. Registration with the Query Server

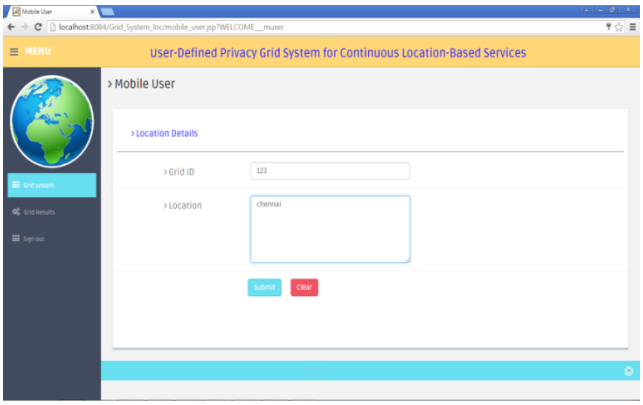

Fig.5. Acquiring the location of the mobile user

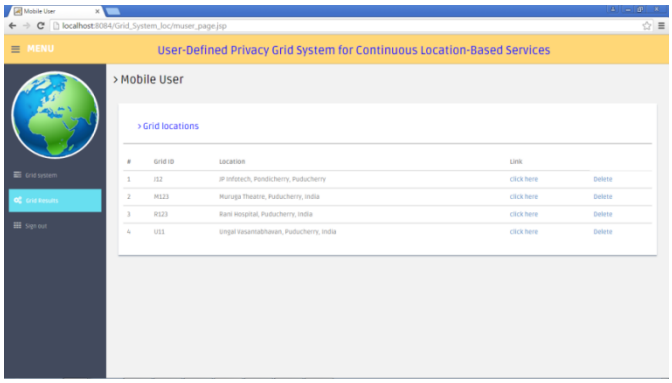

Fig.6. Acquiring the location details in a grid manner

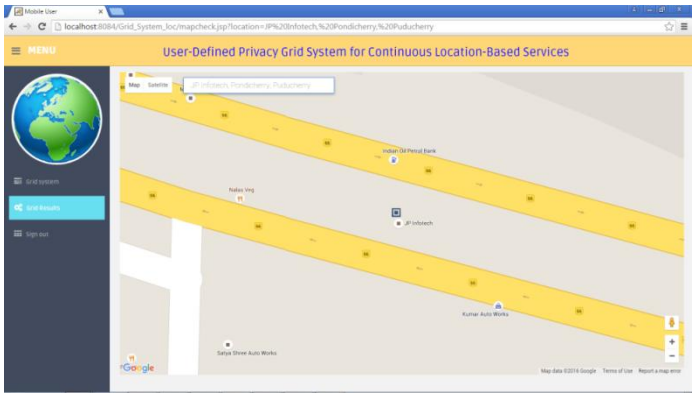

Fig.7. Obtaining the candidate points using distance calculation. Hence the privacy is set.

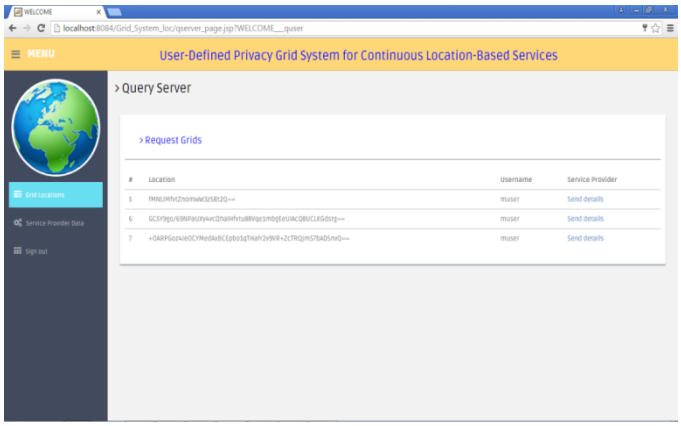

Fig.8. Grid Request from user

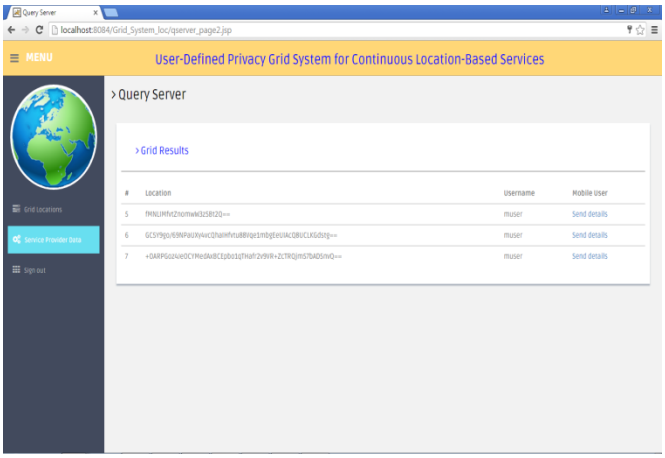

Fig.9. Obtaining the grid results from service provider

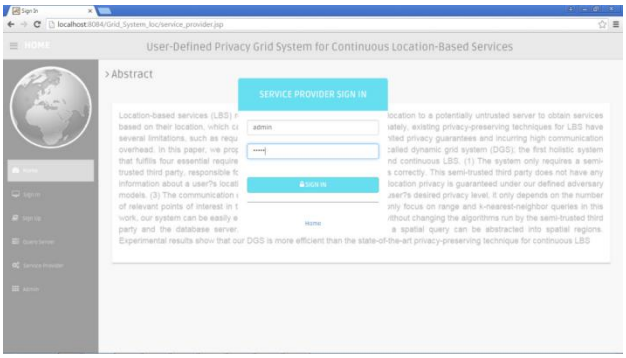

Fig.10. Login of Service Provider

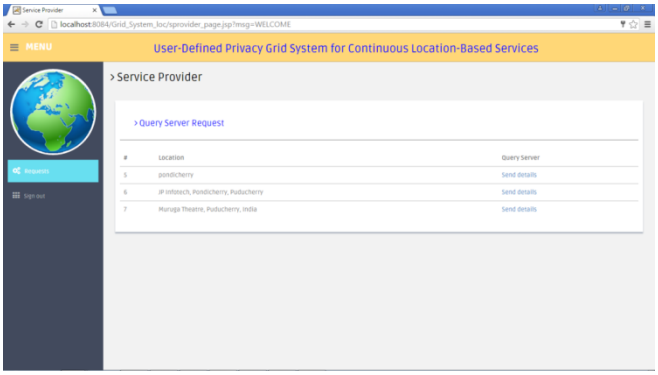

Fig.11. Request from Query Server

REFERENCES

[1] Anonymous Web Surfing. http://www.anonymizer.com.

[2] Platform for Privacy Preferences (P3P) Project. http://www.w3.org/P3P/.

[3] U.S. Geological Survey. http://www.usgs.gov.

[4] C. Aggarwal. On k-Anonymity and the Curse of Dimensionality. In VLDB, 2005.

[5] B. Bamba and L. Liu. Privacy Grid: Supporting Anonymous Location Queries in Mobile Environments. Technical report, Georgia Tech., 2007.

[6] R. Bayardo and R. Agrawal. Data Privacy Through Optimal k-Anonymization. In ICDE, 2005.

[7] A. Beresford and F. Stajano. Location Privacy in Pervasive Computing. Pervasive Computing, IEEE, 2003.

[8] Computer Science and Telecommunications Board. IT Roadmap to a Geospatial Future. The National Academics Press, 2003.

[9] M. Duckham and L. Kulik. A Formal Model of Obfuscation and Negotiation for Location Privacy. In Pervasive, pages 152–170, 2005.

[10] B. Gedik and L. Liu. Location Privacy in Mobile Systems: A Personalized Anonymization Model. In ICDCS, 2005.

[11] G. Ghinita, P. Kalnis, and S. Skiadopoulos. PRIVE: Anonymous Location-Based Queries in Distributed Mobile Systems. In WWW, 2007.

[12] M. Gruteser and D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In MobiSys, 2003.

[13] M. Gruteser and D. Grunwald. Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis. Mobile Networks and Applications, 2005.

[14] J. Hong and J. Landay. Architecture for Privacy-Sensitive Ubiquitous Computing. In Mobisys, pages 177–189, 2004.

[15] K. LeFevre, D. DeWitt, and R. Ramakrishnan. Incognito: Efficient Full-Domain K-Anonymity. In SIGMOD, 2005.

[16] N. Li, T. Li, and S. Venkatasubramanian. T-Closeness: Privacy Beyond k-Anonymity and l-Diversity. In ICDE, 2007.

[17] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam. l-Diversity: Privacy Beyond k-Anonymity. In ICDE, 2006.

[18] M. Mokbel, C. Chow, and W. Aref. The New Casper: Query Processing for Location Services without Compromising Privacy. In VLDB, 2006.

[19] L. Sweeney. Achieving k-Anonymity Privacy Protection Using Generalization and Suppression. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002.

[20] X. Xiao and Y. Tao. Personalized Privacy Preservation. In SIGMOD, 2006.

[21] X. Xiao and Y. Tao. m-Invariance: Towards Privacy Preserving Re-publication of Dynamic Datasets. In SIGMOD, 2007.

[22] 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.