International Journal For Technological Research In Engineering
Volume 2, Issue 10, June-2015 *ISSN (Online): 2347 - 4718*

SECURE LOCATION-BASED QUERY ROUTING BASED ON HOMOMORPHIC ENCRYPTION SCHEME

Shaik Abdul Khaleel[1], R. China Appala Naidu[2]
[1]M. Tech Student, [2]Associate Professor
Department of CSE, St. Martin's Engineering College, Dhulapally village, RangaReddy district, Telangana state, India.

Abstract: In today's times, it's terribly straightforward for someone to understand his/her location with the assistance of devices having GPS facility. When user's location is provided to LBS, it's attainable to user to understand all location dependent data like location of friends or Nearest Restaurant, whether or not or traffic conditions. the huge use of mobile devices pave the method for the creation of wireless networks which will be used to exchange data supported locations. once the exchange of location data is completed amongst entrusted parties, the privacy of the user may well be in harmful. Existing protocol doesn't work on many various mobile devices and another issue is that, Location Server (LS) should offer deceptive knowledge to user. thus we tend to square measure engaged on improvement of this protocol.
Key words: GPS, LBS, Protocol, private information retrieval, oblivious transfer, Homomorphism

I. INTRODUCTION

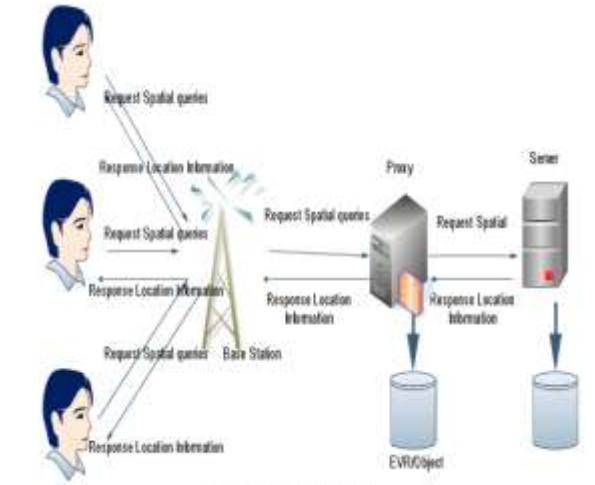
Location based Service (LBS) has been wide used attributable to the explosive preparation of location-detection devices, like sensible phones, world positioning system devices and then on. A LBS information server provides tailored and customized services to users in accordance with their precise location info. An example of such services includes vary question "show Maine a listing of restaurants inside 2km distance from my current location", and nearest neighbor question "where is that the nearest hospital". However, location information is sensitive below some circumstances and users square measure typically unwilling to disclose such info to shady LBS servers as malicious adversaries could acquire a lot of personal data of the victims. Location privacy is explicit information privacy. it's outlined because the ability to stop different unauthorized parties from learning one's current or past location. In location primarily based services, there square measure conceivably two varieties of location privacy: personal subscriber level privacy and company enterprise-level privacy. Personal subscriber-level privacy should offer rights and choices to people to manage once, why, and the way their location is employed by correlate purpose group project-level privacy is basically completely different in this corporate IT managers generally managing once, why, and the manner mobile phone setting capabilities offer application benefits to the organization as an entire. The rest of the paper is organized as follows: Section a pair of reviews the placement privacy in mobile environments; Section three gift privacy molest models. as a final point division five conclude the paper and points out the long run work.

II. RELATED WORK

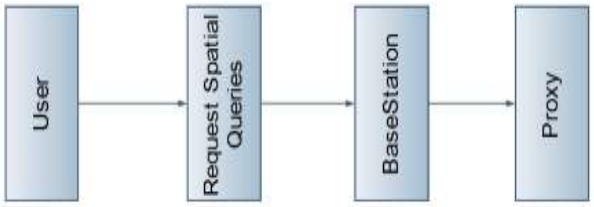
The advent of high-speed wireless networks and therefore the quality of moveable devices have oil-fired the event of cellular phone compute. Distinguished to ancient computing paradigms, mobile computing permits shoppers to own unrestricted quality whereas maintaining network association. the power of users to maneuver and determine their own locations disclose a replacement quite info services, referred to as location-dependent info services (LDISs), which turn out the solution to question per the situation of the consumer supplying the query . Samples of mobile LDISs embody nearest object looking out and native info access, news, and attractions. The spatiality of location-dependent information introduces new issues for information caching analysis. First, the cached result for a question could become invalid once the consumer moves from one location to a different. the upkeep of the validity of the cached information once the consumer changes location is termed location-dependent cache breakup. Second, the cache replacement policy on the consumer has got to consider the sizes of the valid of the cached values. The valid scope of a data worth is outlined because the geographic region at intervals that the information worth is valid. once the valid scope of a knowledge value is giant, the prospect for the consumer to issue constant question at intervals the valid scope, so generating a cache hit, is also large. As such, the cache replacement policy ought to attempt to retain the info worth with pa larger valid scope space in the cache. Owing to increasing demands from mobile users, Location-Based Services (LBSs) have received plenty of attention in recent years. samples of queries for location-based services embody "find the closest petrol station from my current location", "find all the cinemas at intervals one kilo meter radius", "which buses can travel ME within the next ten minutes?" and then on. whereas information objects within the initial 2 examples area unit stationary, those within the last example area unit mobile. during this paper, we focus on queries issued by mobile users on comparatively static information objects, as a result of they\'re the foremost common quite queries in LBSs. The movement of mobile shoppers presents several new analysis issues for location-dependent question processing there area unit many technical problems involved the implementation of associate degree LBS, that embody locating the position of a mobile user, trailing and predicting

movements, process queries expeditiously, and bounding location errors. Consider a computing atmosphere with an outsized range of location-aware mobile objects. we would like to retrieve the mobile objects within a group of user-defined spacial regions and incessantly monitor the population of those windows over a period of time. during this paper, we have a tendency to check with such continuous queries as range-monitoring queries. Efficient processing of range-monitoring queries might change several helpful applications. similarly, we'd wish to trace traffic condition pin some space and dispatch additional police to the region if the amount of vehicles within exceeds a certain threshold. In such applications, it's extremely fascinating and someday vital to produce correct results and update them pin real time whenever mobile objects enter or exit the regions of interest. not like typical vary queries, a range-monitoring question could be a continuous question. It stays active till it\'s terminated expressly by the user. As objects still move, the question results modification consequently and need continuous updates. a straightforward strategy for computing vary observation queries is to own every object report its position because it moves. The server uses this information to spot the affected queries, and updates their results consequently. this easy approach needs excessive location updates, and clearly is n't ascendible. every location update consists of 2 expenses – mobile communication price and server process price. If a powered object has got to perpetually report its location, the battery would be exhausted terribly quickly. it\'s well-known that causation a wireless message consumes considerably more energy than running easy procedures. Mobile devices with process, storage, and wireless communication capabilities (such as PDAs) have become increasingly well-liked. At an equivalent time, the technology behind positioning systems is continually evolving, enabling the integration of low value GPS devices in any moveable unit. Consequently, new mobile computing applications area unit expected to emerge, permitting users to issue location-dependent queries during a present manner. Consider, for instance, a user (mobile client) in Associate in Nursing unknown town, World Health Organization would love to grasp the ten nearest restaurants. This is an instance of a k nearest neighbor (kNN) question, wherever the question purpose is that the current location of the consumer and also the set of data objects contains the town restaurants. instead, the user might kindle all restaurants set inside a particular distance, i.e., inside two hundred meters. this can be Associate in Nursing instance of a spread question. spacial queries are studied extensively within the past, and diverse algorithms exist (for process exposure queries on static knowledge indexed by a spatial access technique. sequent strategies targeted on moving queries (clients) and/or objects. the most plan is to return some further data (e.g., additional NNs termination time validity region that determines the period of the result. Thus, a moving consumer has to issue another question solely when the present result expires. These strategies focus on single question process, ensure assumptions regarding object movement and don\'t embrace mechanisms for maintenance of the question results (i.e., once the result expires, a brand new question should be issued). Recent analysis considers continuous watching of multiple queries over every which way moving objects. during this setting, there's a central server that monitors the locations of each objects and queries. The task of the server is to report and incessantly update the question results because the purchasers and also the objects move. As Associate in Nursing example, take into account that the info objects area unit vacant cabs and also the purchasers area unit pedestrians that would like to grasp their k nearest free taxis till they rent one. As the reverse case, the queries might correspond to vacant cabs, and every free taxi driver desires to be incessantly enlightened regarding his/her k nearest pedestrians. many watching strategies are planned, covering each vary and kNN queries. Some of these strategies assume that objects issue updates whenever they move, whereas others take into account that knowledge objects have some process capabilities, in order that they inform the server only if their movement influences
some query greater.

III. FRAME WORK



Overall system design



Client process flow

Existing work contains 2 protocols specifically oblivious transfer part and personal statistics reclamation .First user in public determines his location mistreatment GPS coordinates then he determines personal location in a very public grid mistreatment oblivious transfer .After obtaining cell id and related regular key from server, user fires question is treatment PIR protocol and obtain correct block from info that he needs. Here there\'s assurance of privacy each for user and server. By learning higher than analysis works by scholar we have a tendency to are going to enhance this

technique. as a result of when user wants to determine his location and in line with that he fires question to the server. therefore there ar surplus steps to done to accumulate block of knowledge from info server. thus we have a inclination to are aim to intend system with range of users in same public grid or region can acquire info mistreatment a single purpose. In existing system, user question to server for his, after that server forward bowl involving to its spot. Here we've taken under consideration an inspiration of CENTROID i.e. in a very explicit region, there are range of unknown users use location primarily based services. therefore for each user, he needs to confirm his location and send it to server. thus we resolute that we will erect only idea surrounded by the expanse for communication with server .So there's no ought to each user to determine its region all the time. The build of midpoint of throng is wholly unusual than previous existing systems. Here we have a tendency to guess that, every one of the user in a open grid proverbial to every alternative i.e. they're sure with each other. Then one among the teams from the general public grid will make a center of mass purpose for communication with server as a result of they have a trust on one an added. therefore one among the sure user in the cluster gain locations of alternative user and build a center of mass point. After computing the center of mass, user sends it to all or any his companion and LBS supplier. therefore actual position of the user and his companions remains hidden. By obtain core of throng all the users fire the difficulty regarding thereto centre purpose. Here we have a tendency to cannot search nearest neighbors question .But user will access information from server from their real location and LBS server wouldn't understand actual point of client and it'll launch information to interior of mass. One advantage therein is we will take restricted range of users from a public grid. All the users are sure and known to every alternative. therefore privacy is will enlarge. likewise we have a inclination to are going to develop this by masking the locations of user and their companions whereas creating a center of mass.

IV. EXPERIMENTAL RESULTS

Performance Analysis:

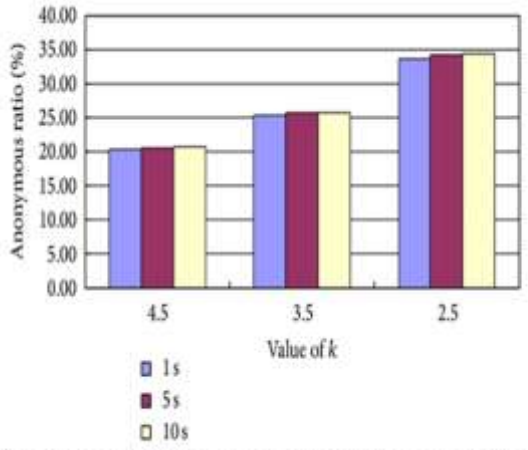
When we are performing operations on our application we have taken the values like below table

TABLE 1

Average service delay request (second)	Average location precision (mile)	Request amount	Average spatial request (k_s)	Average temporal request (k_t)	Minimum radius R_{min} in average anonymous area (mile)	Maximum radius R_{max} in average anonymous area (mile)
1	50.03	466034	4.49	4.50	274.94	637.11
1	50.04	503432	3.50	3.50	275.43	637.43
1	50.08	453293	2.50	2.50	275.18	636.67
5	50.06	457712	4.50	4.50	275.08	637.25
5	49.98	446796	3.50	3.50	275.19	636.99
5	50.01	442778	2.50	2.50	275.12	637.06
10	50.08	456814	4.50	4.50	274.79	637.74
10	49.93	697438	3.50	3.49	275.01	637.54
10	49.98	681948	2.50	2.49	274.84	637.43
10	50.08	493648	2.50	2.50	525.21	1263.51
10	49.97	459932	2.49	2.50	774.50	1307.06
20	49.97	448366	2.50	2.51	275.27	637.64
30	50.03	472418	2.50	2.50	275.37	637.87

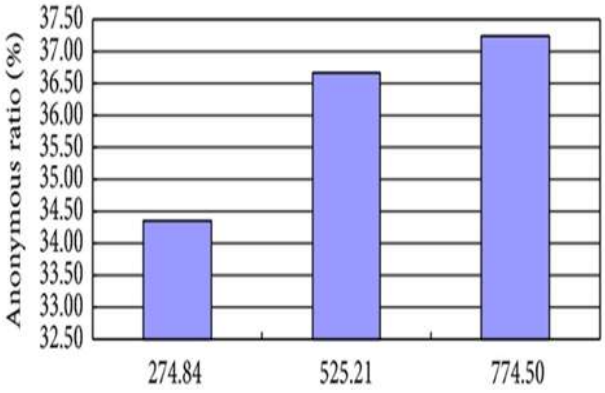
As per the table values the resultant graphs will be like below

i) ratio of the temporal-spatial anonymity with different waiting time and average anonymous request.



Ratio of the temporal-spatial anonymity with different waiting time and average anonymous request.

ii) ratio of the temporal-spatial anonymity with different anonymous space requests.



Ratio of the temporal-spatial anonymity with different anonymous space requests

V. CONCLUSION

In this paper we've got conferred a location based mostly question solution that employs 2 protocols that permits a user to in camera verify and acquire location information. The first step is for a user to in camera verify his/her location using oblivious transfer on a public grid. The second step involves a personal data retrieval interaction that retrieves the record with high communication potency. We analyzed the performance of our protocol and located it to be each computationally and communication ally additional efficient than the answer by Ghinita et al., that is that the most recent resolution. we have a tendency to enforced a software package epitome using a desktop machine and a mobile device. The software package prototype demonstrates that our protocol is inside sensible limits. Future work can involve testing the protocol on several different mobile devices. The mobile result we offer may be totally different than different mobile devices and software package

environments. Also, we want to cut back the overhead of the property check utilized in the personal data retrieval base set of rules. in toting up, the matter regarding the LS supply dishonest information to the consumer is as well interesting. retreat conserve name technique appear a suitable approach to deal with such downside. Once appropriate strong solutions exist for the final case, they will be simply integrated into our approach.

REFERENCES

[1] Um, J.H., et al., "K-Nearest Neighbor Query Processing Algorithm for Cloaking Regions Towards User Privacy Protection in Location-Based Services", Journal of Systems Architecture, vol.58, No. 9, pp. 354-371, 2012.
[2] Ardagna, C.A., et al., Privacy-enhanced location-based access control. Handbook of Database Security, 2008: p. 531-552.
[3] Mokbel, M.F., C.Y. Chow and W.G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy", in Proceedings of the 32nd International Conference on Very Large A Survey of Location-Based Privacy Preserving Gaoming Yang, Jingzhao Li, Shunxiang Zhang, Huaping Zhou 32 Data Bases, VLDB Endowment, 2006.
[4] Krumm, J., "Inference Attacks on Location Tracks", Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 127-143, 2007.
[5] Ardagna, C.A., et al., "Location Privacy Protection Through Obfuscation-based Techniques", Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4602 LNCS, pp. 47-60, 2007.
[6] Mokbel, M.F., C.Y. Chow and W.G. Aref, "The New Casper: A Privacy-aware Location-based Database Server", in IEEE 23rd International Conference on Data Engineering, ICDE 2007, IEEE, 2007.
[7] Ghinita, G., P. Kalnis and S. Skiadopoulos, "PRIVE: Anonymous Location-based Queries in Distributed Mobile Systems", in Proceedings of the 16th international conference on World Wide Web, ACM, 2007.
[8] Chow, C.Y., M.F. Mokbel and X. Liu, "Spatial Cloaking for Anonymous Location-Based Services in Mobile Peer-to-Peer Environments", GeoInformatica, vol. 15, No. 2, pp. 351-380, 2011.
[9] Bamba, B., et al. "Supporting Anonymous Location Queries in Mobile Environments with Privacy grid", in Proceedings of the 17th International Conference on World Wide Web, ACM, 2008.
[10] Gao Rui, Wang Wenjun, et al. "Privacy Preserving Traffic Speed Estimation via Mobile Probe", International Journal of Digital Content Technology and its Applications, vol. 6, no.1, pp.446-453, 2012.
[11] Ghinita, G., et al. "Private Queries in Location Based Services: Anonymizers are not Necessary", in Proceedings of the 2008 ACM SIGMOD international conference on Management of data, ACM 2008.
[12] Liu, W., et al., "A Tree Based Location Privacy Approach Against Multi-Precision Continuous Attacks in the Internet of Things", Journal of Information and Computational Science, vol. 9, No. 7, pp. 1807-1819, 2012.
[13] Xu, J., et al., "Privacy-Conscious Location-Based Queries in Mobile Environments", IEEE Transactions on Parallel and Distributed Systems, vol. 21, No. 3. pp. 313-326, 2010.
[14] Ni, W.W., J.W. Zheng and Z.H. Chong, "HilAnchor: Location Privacy Protection in the Presence of Users' Preferences", Journal of Computer Science and Technology, vol. 27, No. 2. pp. 413-427, 2012.
[15] Khoshgozaran, A., H. Shirani-Mehr and C. Shahabi, "Blind Evaluation of Location Based Queries Using Space Transformation to Preserve Location Privacy", GeoInformatica, pp. 1-36, 2012.

