Privacy Efficient System for Secure Location Based Queries

[1]SANA MARYAM, [2]AMTUL SHANAZ,[3]DR. SYED RAZIUDDIN

[1]M.E Student, Department of CSE, Deccan College of Engineering and Technology, Darussalam Road, Mandal Nampally, Hyderabad, Telangana, India

[2]Assistant Professor, Department of CSE,Deccan College of Engineering and Technology, Darussalam Road, Mandal Nampally, Hyderabad, Telangana, India

[3]Professor and Head of Dept,Department of CSE,Deccan College of Engineering and Technology, Darussalam Road, Mandal Nampally, Hyderabad, Telangana, India

ABSTRACT:

Location-based services (LBS) are a widespread class of computer application-level offerings that use location information to govern capabilities. As such, LBS are a vice. This has come to be increasingly important with the enlargement of the information service and has a wide variety of uses in social networking nowadays as an amusement service, which is available with cell devices through the mobile network and which makes use of information at the geographical position of the cellular the smart phone and tablet markets as properly. LBS consist of parcel monitoring and automobile monitoring services.The Location Server (LS), which offerLBS, assets to bring the statistics approximately diverse exciting POIs. As a result, it is expected that the LS could now not disclose any facts without costs. Therefore, the LBS have to make sure that any unauthorized consumer does no longer get admission to LS's information. For this reason, we develop a protocol to gain consumer and server aspect privacy. Using oblivious transfer and PIR (personal information retrieval) protocols, we obtain secure information for each event. Our scheme is, proven strong so long as the underlying security features have better security strength. Furthermore, we show in a quantitative manner, that the schemes keep almost all the protection of the underlying characteristic. We propose a major enhancement upon previous solutions by introducing a cache. The solution we present isefficient and practical in many scenarios. We implement our solution on a desktop machine and a mobile device to assess the efficiency of our protocol.We offer new structures cache technique to improve work ability of our approach we integrate technique called "in memory cache management" to reduce the response time and bandwidth of data traffic from the location server.

Index Terms - Location based query, private query, private information retrival, oblivious transfer, cache.

I. INTRODUCTION

There are increasing cellular smart phone users worldwide. So location based technologies can be presently utilized by wireless service operators to offer an awesome forecast of the user place. Nowadays, wide variety of customers are use area primarily based offerings which can

provide location-aware facts. Location based service provider is a carrier available with cellular devices, pocket pc's, GPS devices. It's far like Google maps, map request. Mobile gadgets with positioning abilities (e.g. GPS) facilitate get entry to region based offerings that offer statistics relevant to the user's geospatial context. variety of customers uses those offerings for retrieving factors of interest from their contemporary location. LBS may be query based and affords the end user with useful records together with "in which is the nearest restaurant?" basically when user used particular location based service or registered for that, then LBS can provide quantity of other services like transport coupons or other advertising and marketing statistics to purchaser who's in a selected geographical location.

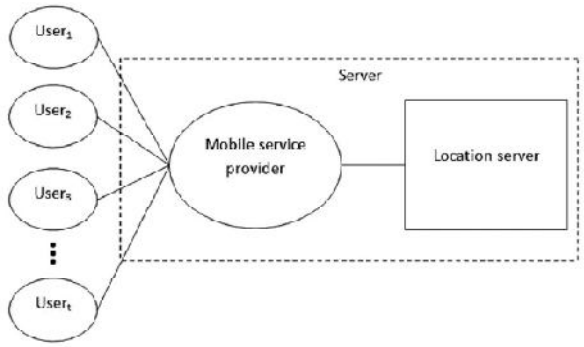

Figure 1: System Architecture

On this paper, we suggest a novel protocol for location based queries that have most important overall performance upgrades with appreciate to the method by Ghinita at el. Like such protocol, our protocol is prepared in step with stages. Within the first stage, the consumer privately determines his/her area within a public grid, by using oblivious transfer. This information incorporates both the identification and associated symmetric key for the block of records in the non-public grid. in the second level, the consumer executes a communicational efficient PIR, to retrieve an appropriate block in the private grid. This block is decrypted the usage of the symmetric key received in the preceding stage.

II. RELATED WORK

Lots of research has been completed on privacy maintaining. However nobody gave absolute guarantee of user's facts and query.Those are:Path Confusing: with the help of path perturbation set of rules that constantly accumulate area sample from a large institution of customers. When customers met at one region, this algorithm can move paths in region. So adversary could confuse the paths of distinctive customers. If users circulate in parallel, the direction perturbation algorithm perturbs the parallel phase into crossing phase. However this set of rules technique is not able to protect time-series place records.

Creating Dummy Locations:This approach in particular employs the concept of dummy locations to shield a person's area privateness. These methods recommend generating dummy trajectories in order to confuse the adversaries. In that once person can question to server with their cellular location and parameters, it may be

transformed into another question having person's real location and k-1 dummy locations and their parameters. However observe that, privateness is not included via changing the actual consumer identity with fake one because in order to system place based queries, the LBS desire the exact place of querying consumer.

Using K-Anonymity: K-anonymity is a extensive-unfold fashionable privacy concept no longer constrained to region privateness. It gives the guarantee that during a set of k items (cellular users), the target object is indistinguishable from the alternative k – 1 items. With this technology it adds one idea ANONYMISER which is trusted third party. A consumer sends its region, query and k to the anonymized, that is a trusted third party in centralized structures or a peer in decentralized systems. The anonymiser eliminates the identification of the person. TTP regenerate cloak for consumer area by using making K-anonymized spatial vicinity wherein number of k-1 customers are worried. Then anonymiser sends the k-ASR and question to the LBS sever, which calculates the candidate results respect to the cloaked area and sends them returned to the anonymizer. Then the anonymiser which knows the locations of all of thecustomers calculates the actual results and sends them back to the consumer.There is a enhancement of this approach that is as a substitute sending all cloaked area to server, an anonymiser only sends a middle of k-anonymizing spatial region (k-ASR). But still there are drawbacks in k-anonymity- (i) If attacker without delay gains the access of anonymiser, the privacy of all users is compromised. (ii) At the least minimal person must subscribe, otherwise CR can't be constructed. (iii) Consumer updating is some other for making clocking regions. (iv) If person fireplace query out of the clocked area, he may be effortlessly recognized because he can be blanketed in all CRs. iv)non-public records Retrieval The simple concept is to hire PIR [12] to allow the consumer to query the location database without compromising the privacy of person .past approach requires clocked area and a TTP, but it doesn't want of anonymiser and privateness is gain thru cryptographic techniques. Here server forms the place regarding to POI and even as answering to question, server first send regions to consumer. The consumer unearths the location that contains him and utilizes PIR to request all points inside that vicinity. So, the server does not recognize which area was retrieved. But this approach is costly and high CPU value. Additionally consumer can go through high preliminary test, so more time required to execute query is more.

III. FRAMEWORK

On this paper, we suggest new kind protocol for location based queries that has fundamental overall performance enhancements with respect to the approach by way of Ghinita at el. Like

such protocol, our protocol is prepared in step with two tiers. Within the first level, the user privately determines his/her location inside a public grid, by using oblivious switch. This data includes both the identity and related symmetric key for the block of information inside the private grid. Within the second stage, the user executes a PIR, to retrieve the precise block inside the private grid. This block is decrypted by using the symmetric key acquired inside the previous level. Our protocol thus gives safety for each the user and the server. The user is included due to the fact the server is not able to determine his/her region. Similarly, the server's information is being protected since a malicious user can handiest decrypt the block of data received through PIR with the encryption key acquired within the preceding level. In other phrases, users can't gain any more records than what they have got paid for. We remark that this paper is an enhancement of a preceding work. Mainly, the subsequent contributions are made. 1) Redesigned the key structure 2) added a proper protection model 3) applied the solution on both a cell device and laptop machine As with our previous work, the implementation demonstrates the performance and practicality of our technique. Our protocol consists of initialization section and transfer section. Now we define procedure required for the stages after which we can officially define the safety of these levels. Our initialization segment is administered by the sender (server), who owns a database of location information data and a 2-dimensional key matrix Km×n, where m and n are rows and columns respectfully. An element in the key matrix is referenced as ki,j. each ki,j in the key matrix uniquely encrypts one document. a fixed of prime powers S, wherein N is the wide variety of blocks, is to be had to the general public. Each detail in S the pi is a prime and ci is a small natural digit such that $p_i^{c_i}$ is greater than the block size (where each block includes some of POI statistics). We require, for convenience that the factors of S follow a predictable pattern. In addition, the server units up a not unusual safety parameter k for the framework.In context of this work we have seen the working of proposed methodology in order to preserve the location privacy of a user form being known to the location server and other kind of users or attackers. Our work can handle the security of data and location privacy in an efficient manner. To further improve work ability of our approach we integrate technique called "***in memory cache management***" to reduce the response time and bandwidth of data traffic from the location server.The system model consists of kinds of entities the set of users1 who wish to access location information, a mobile service company SP, and a location server LS,cache. From the point of view of a person, the SP and LS will com-pose a server, to be able to serve both functions. The person does no longer need to be involved with the specifics of the communication. The customers in our version use a few location-based service supplied by means of the location data server

LS. Here is an architecture of our enhanced cache model.

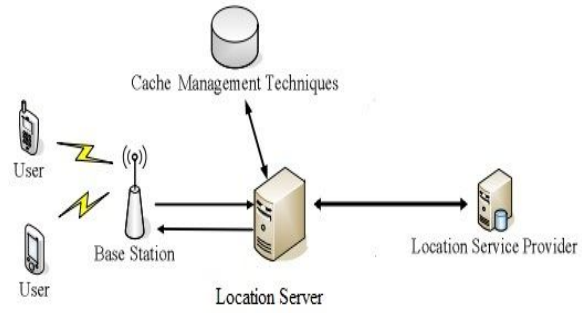

Figure2: Proposed System Architecture

Our in memory cache enabled initially when the user passes a location request to the server. A request from the user is taken by cache of the system and verified that weather the request data is available in cache or not. If a request is found, a user obtains the response from cache; in case a request not found in cache then we transfer the request to the location service provider. This can improve the work efficiency and response of the system. With the help of cache manage a user get the information if he/she is not connected to the network.

IV. EXPERIMENTAL RESULTS

We have been developed our location based query system on a platform along with: a desktop system, running the server software program of our protocols; and a mobile device, executing the user software program of our protocols. For each platform, we measured the desired time for the oblivious transfer and personal data retrieval protocols and cache one after the other to check the performance of each protocol and the relative work ability among the protocols.

V. CONCLUSION

In this paper, we have discussed a location based query solution that employs protocols that allows a user to privately obtain and gather their personal location. At first the user has to privately decide his/her location by making use of oblivious transfer on a public grid. The subsequent step entails a private data retrieval interaction that retrieves the report with excessive communication performance. To conclude, cache management techniques which can be efficient.Significantly, our solution can further improve user privacy protection, save computational resources, and decrease communication costs. However, both the queryprocessing time and communication costs can beeffectively decreased.

REFERENCES:

[1] A. Beresford and F. Stajano, “Location privacy in pervasive computing,” IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, Jan.–Mar. 2003.

[2] C. Bettini, X. Wang, and S. Jajodia, “Protecting privacy against location-based personal identification,” in Proc. 2nd VDLB Int. Conf. SDM, W. Jonker and M.

Petkovic, Eds., Trondheim, Norway, 2005, pp. 185–199, LNCS 3674.

[3] X. Chen and J. Pang, "Measuring query privacy in location-based services," in Proc. 2nd ACM CODASPY, San Antonio, TX, USA, 2012, pp. 49–60.

[4] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," J. ACM, vol. 45, no. 6, pp. 965–981, 1998.

[5] M. Damiani, E. Bertino, and C. Silvestri, "The PROBE framework for the personalized cloaking of private locations," Trans. Data Privacy, vol. 3, no. 2, pp. 123–148, 2010.

[6] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in Proc. 3rd Int. Conf. Pervasive Comput., H. Gellersen, R. Want, and A. Schmidt, Eds., 2005, pp. 243–251, LNCS 3468.

[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inform. Theory, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[8] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in Proc. ICDCS, Columbus, OH, USA, 2005, pp. 620–629.

[9] C. Gentry and Z. Ramzan, "Single-database private information retrieval with constant communication rate," in Proc. ICALP, L. Caires, G. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, Eds., Lisbon, Portugal, 2005, pp. 803–815, LNCS 3580.

[10] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "A hybrid technique for private location-based queries with database protection," in Proc. Adv. Spatial Temporal Databases, N. Mamoulis, T. Seidl, T. Pedersen, K. Torp, and I. Assent, Eds., Aalborg, Denmark, 2009, pp. 98–116, LNCS 5644.

[11] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearestneighbor queries with database protection," GeoInformatica, vol. 15, no. 14, pp. 1–28, 2010.

[12] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in Proc. ACM SIGMOD, Vancouver, BC, Canada, 2008, pp. 121–132.

[13] G. Ghinita, C. R. Vicente, N. Shang, and E. Bertino, "Privacypreserving matching of spatial datasets with protection against background knowledge," in Proc. 18th SIGSPATIAL Int. Conf. GIS, 2010, pp. 3–12.