ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An efficient Privacy Preserving and Content Protecting and Search by using Points of Interest

Gottumukkala Bindu Madhavi
M.Tech Student
Department CSE,
D.N.R. College of Engineering
& Technology.

M.S.V.V.Ramesh
Assistant Professor,
Department CSE,
D.N.R. College of Engineering
& Technology.

DDD.Suri Babu
HOD & Associate Professor,
Department CSE,
D.N.R. College of Engineering
& Technology.

Abstract:

In today's modern world, it is very easy for a person to know his/her location with the help of devices having GPS facility. When user's location is provided to LBS, it is possible to user to know all location dependent information like location of colleges, restaurants and their related information. The massive use of mobile devices pave the way for the creation of wireless networks that can be used to exchange information based on locations. When the exchange of location information is done amongst entrusted parties, the privacy of the user could be in harmful. Existing protocol doesn't work on many different mobile devices and another issue is that, Location Server (LS) should provide misleading data to user. So we are working on enhancement of this protocol.

Keywords:

Location Privacy, Private Information Retrieval, Location Server, Mobile Service Provider.

I.INTRODUCTION:

An entertainment and utility service, generally accessible Location Based Service (LBS) have become an immensely valuable source of real-time information and guidance. Location-based services (LBS) are a general class of computer program-level services that use location data to control features. As such LBS is an information service and has a number of uses in social networking today as an entertainment service, which is accessible with mobile and operating through a mobile network, which uses information on the geographical position of the mobile device. Location based queries are provided by location based service (LBS). These are generally based on a point of interest (POIs). By retrieving the Points Of Interest from the database server, user probably get answers to various location based queries, which are for example discovering the hospital, ATM machine or police station, restaurant. In years there has been increase in the number of devices querying location servers for information about POIs. Queries are thus use for obtain required information from database.

Location Based Service (LBS):

Location based service is a service accessible with mobile phones, GPS devices, pocket PCs,. It is like Google maps, map request. A mobile device with positioning capabilities (e.g. GPS) facilitates access to location based services that provide information relevant to the user's geospatial context. Number of users uses these services for retrieving Points of Interest from their current location. LBS can be query based and provides the end user with useful information such as "Where is the nearest restaurant?"But there are certain problems while using LBS that it may collect and use vast amount of information about consumer for a wide range of purpose. Location information is sensitive and users don't want to share such information to untrustworthy LBS servers. Because number of malicious adversaries may obtain more private knowledge of the users.Also, queries fire by the user having sensitive information about individuals, including health condition, lifestyle habits. So he doesn't want to disclose it. Privacy concerns are expected to rise as LBSs become more common. Location privacy means data privacy. So here privacy assurance is measure issue. On the other, location server has their own database in which, number of point of interest records are located. So server has to prevent database access from unauthorized user and also user who have not pay for that service.

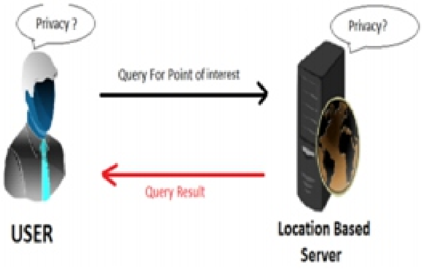


Fig 1 - Location Based Service

Basically the Location Server (LS), which offers some LBS, spends its resources to compile information about various interesting POIs. Hence, it is expected that the LS would not disclose any information without fees. Therefore the LBS has to ensure that LS's data is not accessed by any unauthorized user. During the process of transmission the users should not be allowed to discover any information for which they have not paid. It is thus crucial that solutions be devised that address the privacy of the users issuing queries, but also prevent users from accessing content to which they do not have authorization.Number of Existing system used protocols for privacy of Location based services. But we have to secure three things

i) location privacy
ii) query privacy
iii) database privacy

II.Related Work:

Location Privacy Protection. There are two main approaches to protecting location privacy in LBS. The first approach relies on a trusted LBS server to restrict access to location data based on rule-based policies. The second category of approaches run a trustworthy agent between the client and the LBS server. Every time the user makes a location-based query, the agent anonymizesthe user identity and/or location before forwarding the query to the LBS server. Ourstudy falls into the second category.

K-Anonymity:

K-anonymity is a wide-spread general privacy concept not restricted to location privacy. It provides the guarantee that in a set of k objects (mobile users), the target object is indistinguishable from the otherk –1 objects. With this technology it adds one concept ANONYMISER which is trusted third party. A user sends its location, query and K to the anonymiser, which is a trusted third party in centralized systems or a peer in decentralized systems.

The anonymiser removes the ID or encrypts details of the user. Then anonymiser sends the K-ASR and query to the LBS sever, which calculates the candidate results respect to the cloaked region and sends them back to the anonymizer. Then the anonymiser which knows the locations of all the users calculates the actual results and sends them back to the user. There is a enhancement of this system that is rather sending all cloaked region to server, an anonymiser only sends a center of K-anonymizing spatial region (K-ASR). The basic idea is to employ PIR to enable the user to query the location database without compromising the privacy of user.

III.SYSTEM MODEL AND PROBLEM FORMULATION:

We denote every person engaged in the protocol as a user Ui (we do not differentiate smartphone users and PC users), the user queries the location information of other user as a querier Qi.. When he queries on others, he acts as a querier and when he is queried. That is, Ui = Qi for the same i. We assume an independent semi-honest model for users and service providers. That is, they all behave independently and will try to extract useful information from the anonymizer, We further assume that every user communicate with server via an anonymized network such that the privacy is not compromised by the underlying network protocol. We assume the origin of a packet is successfully hidden, which is out of this paper's scope (otherwise any attacker can achieve the location based on the origin of the packet).

PROBLEM STATEMENT:

The problems of Location Based Service such as a user wants to query a database of location data, known as Points Of Interest (POIs), and does not want to reveal his/her location to the server due to privacy concerns; And also the owner of the location data, that is, the location server, does not want to simply distribute its data to all users.

IV.BACK GROUND:
Base64 Algorithm

Base64 is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation.

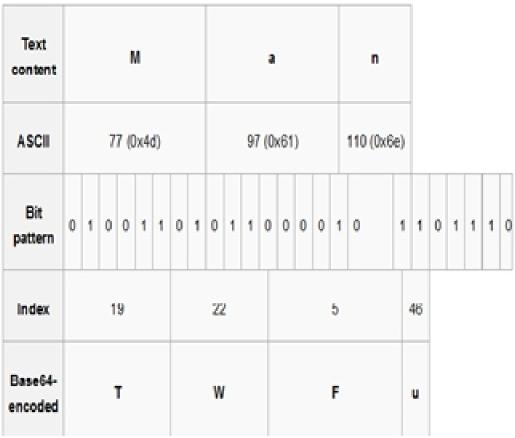
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Base64 encoding works directly on the underlying binary representation of data. It does not really base64 encode strings, the base64 encode the bytes representing the characters that make up strings. Each character in the string is represented by a single 8-bit byte; each character in a base64-encoded string is made up of just 6 bits. Base64 encoding is really nothing more than performing this conversion.There are 65 possible characters in the base64 alphabet: the letters A through Z, a through z, the numbers 0 through 9, the plus sign (+) and the slash (/).

The 65th character is the equals sign (=) and that is used to indicate padding (discussed later). The 6-bit number 0 therefore is represented by the letter A in a base64-encoded string, the 6-bit number 1 is represented by B, and so on.In order to base64 encode data, you need at least 24 bits (the smallest number that's equally divisible by 6 and 8), so any three-character ASCII sequence can cleanly be encoded in base64. Consider the string "hat". The letter "h" is represented by 104 or 01101000 in binary, "a" is 97 or 01100001, and "t" is 116 or 01110100. If you put together, you end up with:

Example

The word MAN is encrypted to TWFU



Text content	M	a	n	
ASCII	77 (0x4d)	97 (0x61)	110 (0x6e)	
Bit pattern	0 1 0 0 1 1 0 1	0 1 1 0 0 0 0 1 0	1 1 0 1 1 1 0	
Index	19	22	5	46
Base64-encoded	T	W	F	u

Fig 2.Example for Algorithm

V.OUR WORK:

Existing work contains two protocols namely oblivious transfer phase and private information retrieval First user publicly determines his location using GPS coordinates and then he determines private location in a public grid using oblivious transfer. After getting cell id and related symmetric key from server, user fires query using PIR protocol and get proper block from database which he wants. Here there is assurance of privacy both for user and server.

* In this paper, we propose a novel protocol for location based queries that have major performance improvements. Our protocol is organized, as the server can activate the valid users. Then those users are acts as authorized users. These authorized users only able to access the service of the Location Based Queries. The Location details are managed by the server. Here Server plays a vital role to provide Details of Location. Unauthorized users can't able to access the Locations.
* It provides protection for both the user and the server. The user is protected because the server is unable to determine his/her location. Similarly, the server's data is protected since unauthorized users can't get the details of the Location.

ADVANTAGES OF PROPOSED SYSTEM:

•Added a formal security model.
•Improved User and Server privacy protection.
•Proposed cache management techniques.
•Presenting basic information of the Location.
•Giving rankings to the Location based on its searching rate.
•Implemented the solution on both a mobile device and desktop machine.

ARCHITECTURE:

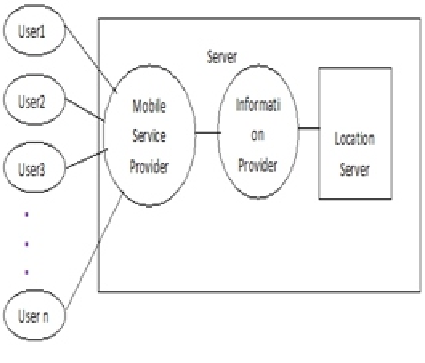


Fig. 3 System Architecture

MODULES DESCRIPTION

Module 1:

Admin

The Admin in our model acts a major part in the system. Admin can control the user's activities by activating or deactivating the users whenever they registered to our model.Admin can add the products to the system .The product details includes Location name, Location Details, Famous for, related image,URL ,Location Map. Etc.Admin can also update the details of the existing Product.

Module 2:
User:

The users in our model use some location-based service provided by the location server. For example, User can enter a query related to the product. Then the User can get the details of the search Product which is existed in the server.

VI.EXPERIMENTAL RESULTS:

To evaluate the performance of our approach, we have implemented our cached based query solutions and cache management mechanisms within a simulator. The objective of our design is to decrease the number of queries which have to be forwarded to service providers to preserve mobile users' privacy, save computational power, and decrease communication costs. Based on our novel cache replacement policies, the cache hit rate can be effectively increased.

Simulator Implementation:

Our simulator consists of four main components, the mobile environment, the location cloaker, the cache management module, and the location-based service provider. For the mobile environment, we applied the network-based moving objects generation framework to generate a set of mobile users and the underlying road network inside the city boundary of Oldenburg in Germany. Each mobile user is an independent object which encapsulates all its related parameters (e.g., its current speed and destination). We implemented our query processing and cache management techniques as new modules for interacting with mobile users to improve query performance and privacy protection. Every simulation has numerous intervals (whose lengths are Poisson distributed), and during each interval, the simulator selects a random subset of mobile users to launch spatial queries (the query intervals are also based on the Poisson distribution). The subset size is controlled by the user defined mean number of queries per minute (e.g., 1000 queries per minute).

To obtain results that closely correspond to realworld conditions, we obtained our simulation parameters from public data sets, for example, mobile user and gas station densities in Oldenburg.

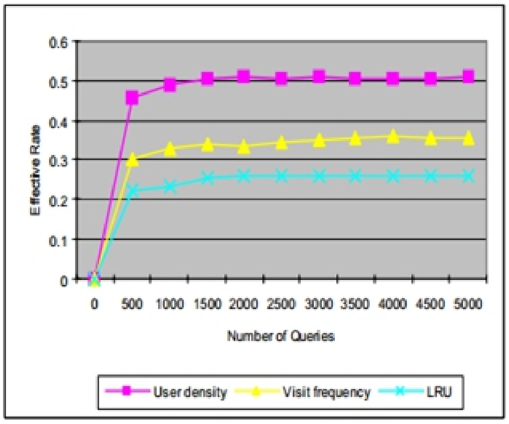


Fig.4The cache hit ratio of the three cache replacement policies with increasing kNN query number.

• Points of Interest: We obtained the information concerning the density of the ofinterest objects (e.g., gas stations, restaurants, etc.) in Oldenburg from Google Maps. Because gas stations are commonly the target of spatial queries, we use them as the sample POI types for our simulations. According to Google Maps, there are 1,399 gas stations inside the city boundary of Oldenburg. Performance of the kNN Query We first tested the performance of our three cache replacement policies with k nearest neighbor query. We increased the number of queries per time interval from 1 to 5000. The cache replacement policy based on mobile user density prevails over two other strategies. The cache hit ratios of our two novel replacement policies are remarkably higher than the traditional LRU solution.

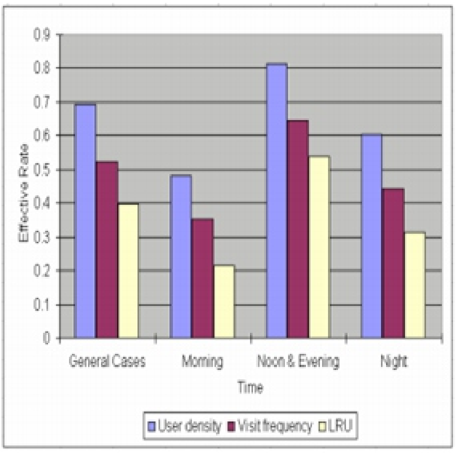


Fig5 .The cache hit ratio of different time intervals during a day with our dynamic cache space allocation mechanism.

Above figure shows the effect of our temporal dynamic cache space allocation mechanism. Our technique improved the cache hit rate for one time interval, Noon & Evening. However, there was no improvement in other two time intervals. Since mobile users' behavior varies at different locations, users may decide when to apply our mechanism based on statistics and experimental results.

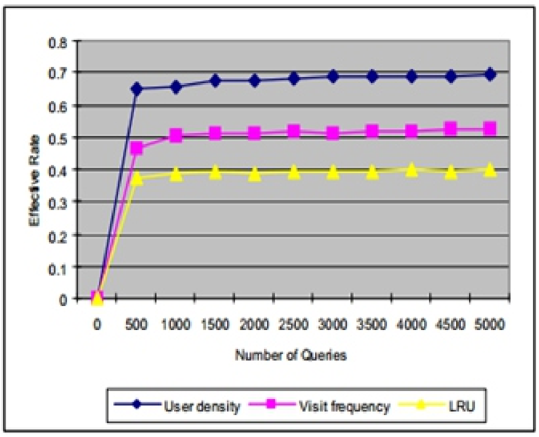


Fig6 The cache hit ratio of the three cachereplacement policies with increasing window query number.

Performance of Window Query:

To see the effect of our cache replacement policies on window queries, we increased the query number from 1 to 5000 and the result is demonstrated in figure 6. Similar to kNN query, the cache replacement policy based on mobile user density outperforms two other strategies and the performance of our two solutions arebetter than LRU.

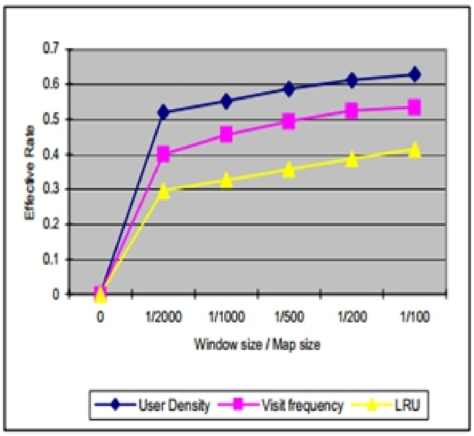


Fig7.The cache hit ratio of the three cache replacement policies with increasing query window

We also studied the effect of various query window sizes by enlarging the query window size from 0 to 1/100 of the whole search space and the results are shown in Figure 7. Basically, the result trend is very similar to the previous experiment.

VII CONCLUSION AND FUTURE WORK:

In today's world, privacy has proved to be major concern. Sensitive information is preserve by people and there is always worry about not allowing it to be share in process of querying. This paper thus put forth survey on existing literature and techniques used in field of privacy for protection of data and other content. Working with privacy preserving, various different techniques used are studied in paper along with their pros and cons. All methods implemented new approach of working in order to satisfy objective is reviewed. The proper maintenance of privacy and the detection of the query that violate privacy is the aim to look upon in process of transfer and retrieval of data between user and server. Based on this future work could be done in efficient way and faster in much more real time. This could be contribution to the system further.

REFERENCES:

[1] Russell Paulet, Md. GolamKaosar, Xun Yi, and Elisa Bertino," Privacy-Preserving and Content-Protecting Location Based Queries", IEEE Transactions on knowledge and data engineering, VOL. 26, NO. 5, MAY 2014.

[2] B. Hoh and M. Gruteser, "Protecting location privacythrough path confusion," in Proc. 1st Int. Conf. SecureComm, 2005,pp. 194–205.

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

[4] B. Gedik and L. Liu, "Location privacy in mobile systems: A per-sonalizedanonymization model," inProc. ICDCS, Columbus, OH, USA, 2005, pp. 620–629.

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

[6] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "A hybrid technique for private location-based queries with database pro-tection," 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.

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

[8] Deepika Nair, BhuvaneswariRaju "Privacy Preserving in Participatory Sensing" in IJSR,Volume 3 Issue 5, May 2014

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

[10] L. Sweeney, "k-Anonymity: A model for protecting privacy," Int. J. Uncertain. Fuzziness Knowl. Based Syst., vol. 10, no. 5, pp. 557–570, Oct. 2002

[11] A. Beresford and F. Stajano, "Location privacy in pervasive com-puting,"IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, Jan.–Mar.2003.

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