ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

PRIVACY PRESERVING QUERY RETRIVAL BASED ON EXTENDED MATRIX ALGORITHM IN LOCATION BASED SERVICES

K.RAJATHI (1), G.MANI RAJ (2)
(1) PG Scholar, CSE Department, SRM University, Chennai
(2) Asst Professor in CSE Department, SRM University, Chennai

Abstract-Now a days, almost every users using LBS (Location Based Services) to get the details about their nearest point of interest. Users will request their POI to LBS and it will process their query based on user's current location. The information collected from the user sometimes reveal sensitive information about the user. There will be a chance of misusing that information. Here we propose a solution for the users to preserve their data privacy and location privacy by using Extended Matrix query retrieval algorithm .This solution allows user to retrieve information from database server without revealing what is actually being requested by the user and retrieved from the server. Compared with existing solutions for kNN quires in Location Based Services, our solution improves the efficiency and security.

Index Terms: Location Based Service, Point of Interest, Extended Matrix, kNN queries

I. Introduction

Location Based Service provider process spatial queries based on user's current location. It will collect the location details and return user requested nearby Point of Interest .Collected location information sometimes reveals some sensitive information about user. There will be chances of misusing those details. Location information is sensitive and users don't want to share such information to untrustworthy LBS servers. Also, queries fire by the user having sensitive information about individuals, including health condition, lifestyle habits. So he/she doesn't want to disclose it. Privacy concerns are expected to rise as LBS become more common. Location privacy means data privacy. So here privacy assurance is major issue. . LBS query based on Extended Matrix provide strong cryptographic guarantees. In this paper, we construct solutions for kNN queries on the basis of Extended Matrix algorithm which will give both data and location privacy

II. Related Work

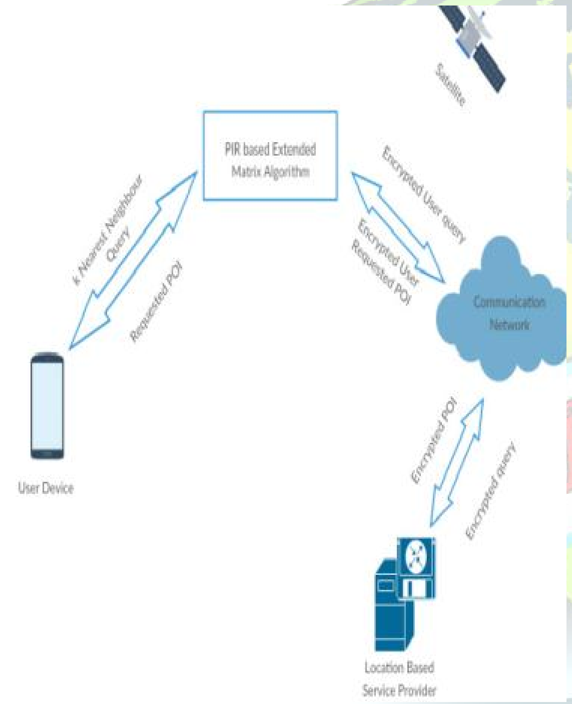
A lot of research has been done on privacy preserving. But no one gave absolute guarantee of user's data and query.

Path Confusion: With the help of path perturbation algorithm that continuously collect location sample from a large group of users. When two users met at one location, this algorithm can employs the idea of dummy locations to protect a user's location privacy. These methods propose to generate dummy trajectories in order to confuse cross paths in area. So adversary would confuse the paths of different users. If two users move in parallel, the path perturbation algorithm perturbs the parallel segment into crossing segment. But this algorithm technique is unable to protect time-series location

Dummy Locations : This method mainly the adversaries. In that when user can query to server with their mobile location and parameters, it can be converted into another query having user's real location and k-1 dummy locations and their parameters. But observe that, privacy is not protected by replacing the real user identity with fake one because in order to process location dependent queries, the LBS needs the exact location of querying user.

Our Extended Matrix solution provides both data and location privacy and improve the efficiency and security information. [7] discussed about creating Obstacles to Screened networks. In today's technological world, millions of individuals are subject to privacy threats. Companies are hired not only to watch what you visit online, but to infiltrate the information and send advertising based on your browsing history.

III.System Architecture


Satellite
PIR based Extended Matrix Algorithm
k Nearest Neighbour Query
Requested POI
Encrypted User query
Encrypted User Requested POI
Communication Network
User Device
Encrypted POI
Encrypted query
Location Based Service Provider

- The mobile user sends location based queries to the LBS provider and receives location-based service from the provider.
- The LBS provider provides location-based services to the mobile user.
- The base station bridges the mobile communications between the mobile user and the LBS provider.
- Satellites provide the location information to the mobile user.

IV. Protocol Description

Extended Matrix Attribute based Encryption Algorithm:

The proposed Extended-Matrix *Based* Query Retrieval, for improving the efficiency and security for nearest neighbor object. Proposed technique takes only two round communications for query retrieval. The normal concept of EMABE is to retrieve a small subset of the content set Pas the set of anchor objects and then assign each object of P to its nearest anchor. For each object p, we evaluate its distance dist (ai, p) from its anchor ai and then apply an order-preserving encryption function OPE on the distance value. These order-preserving encrypted distances will be stored in the server and utilized for processing NN queries.

The transformation key consists of an encryption Key CK, an integer A, and A pairs of the form (ai; ri), where ai is an (anchor) object and ri is a distance value. We will soon elaborate on how to generate the transformation key.

Next, we examine each anchor object. Let ai denote the ith anchor object and the set ai:S represent its assigned set of objects. We compute the anchor's covering radius ri, which denotes the maximum distance from ai to any object in its set ai:S. The anchor distance plays an important role in query processing, as we will discuss shortly. For each object p in the set ai.S, we compute its distance dist(ai, p) from its anchor, and we then apply an order-preserving encryption function OPE on dist(a_i, p). A tuple consisting of the object ID p:id, the order-preserving encrypted distance OPE(dist(ai; p)), and the encrypted object ECR(p, CK) will be sent to the server. The benefit of using OPE is that it hides the original distance values and yet allows comparisons to be correctly evaluated at the server side. Mobile objects can first tune to the air channel, based on which cell they are in, they can follow the pointer and download the query results. Since the query results are meant for the cell, mobile objects will need to refine the results to meet their needs.

KKN Algorithm:

The KNN algorithm is a method for classifying objects based on closest training examples in the feature space. KNN is a type of instance-based learning where the function is only approximated locally and all computation is deferred until classification. In KNN, an object is classified by a majority vote of its neighbours, with the object being assigned to the class most common amongst its K nearest neighbours (K is a positive integer, typically small). If K = 1, then the object is simply assigned to the class of its nearest neighbour. The neighbours are taken from a set of objects for which the correct classification is known. This can be thought of as the training set for the algorithm, though no explicit training step is required.

V. Modules

- User
- Service Provider
- System Model
- PROFIL*R*
- Spotter
- Location Correctness

Users:

The users in our model use some location-based service provided by the location server LS. For example, what is the nearest ATM or restaurant? The purpose of the mobile service provider SP is to establish and maintain the communication between the location server and the user. The location server LS owns a set of POI records ri for 1≤ri ≤ρ. Each record describes a POI, giving GPS coordinates to its location (xgps,ygps), and a description or name about what is at the location.

Service Provider:

We reasonably assume that the mobile service provider SP is a passive entity and is not allowed to collude with the LS. We make this assumption because the SP can determine the whereabouts of a mobile device, which, if allowed to collude with the LS, completely subverts any method for privacy. There is simply no technological method for preventing this attack. As a consequence of this assumption, the user is able to either use GPS (Global Positioning System) or the mobile service provider to acquire his/her coordinates.

System Model

- In this module, we introduce the problem of computing location centric profiles (LCPs) while simultaneously ensuring the privacy and correctness of participants.
- We consider a core functionality that is supported by the most influential geo-social network (GSN) providers
- The provider supports a set of businesses or venues, with an associated geographic location (e.g., restaurants, yoga classes, towing companies, etc). Users are encouraged to report their location, through *check-ins* at venues where they are present. During a check-in operation, performed upon an explicit user action, the user's device retrieves its GPS coordinates, reports them to the server, who then returns a list of nearby venues. The device displays the venues and the user needs to choose one as her current check-in location.
- Then, we propose a venue centric PROFIL*R*, that relieves the GSN provider from a costly involvement in venue specific activities. To achieve this, PROFIL*R* stores and builds LCPs at venues.
- Furthermore, it relies on Benaloh's homomorphic cryptosystem and zero knowledge proofs to enable oblivious and provable correct LCP computations. We prove that PROFIL*R* satisfies the introduced correctness and privacy properties.

PROFIL*R*

- Propose PROFIL*R*, a framework for computing LCPs. Devise both a venue centric and a decentralized solution.
- Prove that PROFIL*R* satisfies the proposed privacy and correctness properties.
- In this section we propose a solution, that when used in conjunction with Sybil detection tools, mitigates this problem.
- No identifying information is sent by users during the *Spotter* and *Check In* procedures: the pseudonyms are *blindly* signed by *S*, all communication with *S* takes place over an anonymizer, and all communication with a venue is done using randomly chosen MAC and IP addresses.

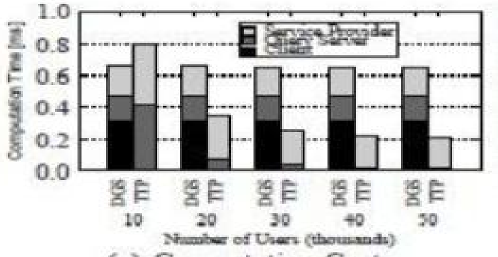
Spotter

- Let *L* and *T* denote *U*'s location and current time. To ensure anonymity, *U* generates fresh random MAC and IP addresses. These addresses are used for a single execution of the *Spotter* and *Check In* protocols. SPOTR*V* uses one of the location verification procedures proposed to verify *U*'s presence at *L* and *T*.
- For simplicity of presentation, we have avoided the Sybil attack problem: participants that cheat through multiple accounts they control or by exploiting the anonymizer.

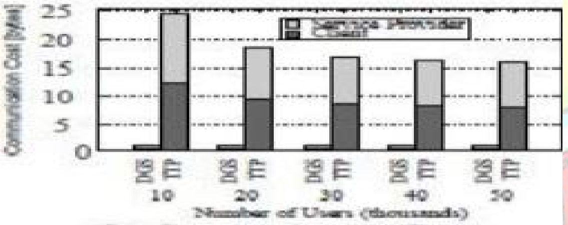
Location Correctness

- The user's location is verified in the *Spotter* protocol. A malicious user not present at venue *V*, is unable to establish a connection with the device deployed at *V*, SPOTR*V* .
- Thus, the user is unable to participate in the challenge/response protocol and receive at its completion a provider signed share of the Benaloh secret key. Without the share, the user is unable to initiate the *Check In* protocol.
- We use one of the protocols proposed to verify the location claims of users checking-in. For completeness, we now briefly describe this protocol. Let SPOTR*V* denote the device installed at venue *V*. When a user *U* expresses interest to check-in at venue *V*, SPOTR*V* initiates a challenge/response protocol.

VI. Performance Evaluation



(a) Computation Cost



(b) Communication Cost

VII. Conclusion

In this paper, we used Extended matrix and kNN protocols to provide Location, Query and Data privacy of user without disclosing any user's details to Location Based Service provider. We analyzed the performance of our protocol and found it to be both computationally and communication ally more efficient than the existing solutions. We have implemented our solution on desktop machines and our future work is to implement on mobile devices.

VIII. References

[1] Xun Yi, Russell Paulet, Elisa Bertino,Vijay Varadharajan-Practical Approximate k Nearest Neighbor Queries with Location and Query PrivacyDOI 10.1109/TKDE.2016.2520473

[2] M. Bellare and P. Rogaway. Optimal asymmetric encryption - how to encrypt with RSA. In Proc. Eurocrypt 1994.

[3] B. Bamba, L. Liu, P. Pesti, and T. Wang. Supporting anonymous location queries in mobile environments with PrivacyGrid. In Proc. WWW 2008.

[4] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. IEEE Pervasive Computing 2(1), 2003.

[5] C. Y. Chow, M. F. Mokbel, and X. Liu. A peer-to-peer spatial cloaking algorithm for anonymous location-based services. In Proc. ACM GIS 2006.

[6] T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory 31 (4): 469-472, 1985.

[7] Christo Ananth, P.Muppidathi, S.Muthuselvi, P.Mathumitha, M.Mohaideen Fathima, M.Muthulakshmi, "Creating Obstacles to Screened networks", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Issue 4,July 2015, pp:10-14

[8] C. Gentry and Z. Ramzan. Single-database private information retrieval with constant communication rate. In Proc. ICALP'05, pages 803-815, 2005.

[9] 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 2008.